




CWID 2008 FINAL REPORT

Assessment Briefs Contents

USJFCOM ENDORSEMENT

Published by: CWID JMO
Edited by: CWID JMO Hampton, VA
For information or to obtain copies, contact: CWIDPA@langley.af.mil
www.cwid.js.mil

CWID 2008 FINAL REPORT ASSESSMENT BRIEFS

Executive Summary

CWID is the Chairman of the Joint Chiefs of Staff-directed annual event that engages cutting-edge information technology focused on criteria defined by combatant commanders. Technologies approved for CWID 2008 participation addressed a new information sharing capability or provided improvements to an existing capability in support of articulated demonstration objectives released as a Federal Business Opportunity (FBO) announcement in April 2007 (www.fedbizopps.gov).

The demonstration evaluated technologies and capabilities for exchanging information among coalition partners, military services, government agencies, first responders and U.S. combatant commanders, especially this year's host, U.S. European Command (USEUCOM). Information sharing technologies leverage decision-making and operational flexibility on the battlefield and during crisis response on the home front.

Everyone involved, commercial and government sectors, took some risk to realize potential benefits. Technology developers brought hardware, software and package solutions to the CWID venue for evaluation. Combatant commands, services, DoD and other government agencies investigated new and emerging technologies, employing the CWID scenario and controlled operational environment for low-threat analysis.

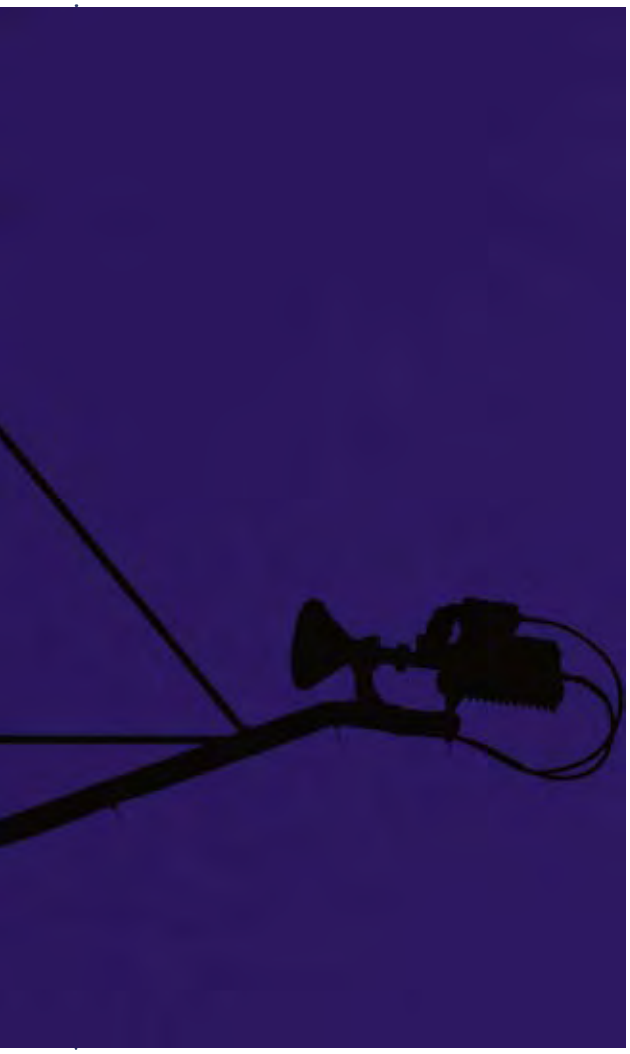
While the CWID 2008 focus was on innovative commercial solutions and emerging technologies, it also provided an annual venue for government information technology development or validation of fielded or near-fielded commercial, DoD and partner systems.

Coalition participation remains the cornerstone of CWID. Interoperability trials with coalition partners are hosted over a worldwide secure network, enabling classified, releasable data to be exchanged among Canada, New Zealand, United Kingdom, NATO, and Partnership for Peace nations.

Information sharing technologies leverage decision-making and operational flexibility on the battlefield and during crisis response on the home front.

Depending on demonstrated capabilities and based on planning-documentation criteria, each information technology trial received one or more assessments: Warfighter/Operator; Technical/Interoperability; and Information Assurance. The Systems Engineering and Integration Working Group (SEIWG), with input from other working groups, reported on interoperability trials not formally assessed by the Assessment Working Group (AWG). Assessment results and SEIWG evaluation reports are documented within this final report.

The CWID JMO consolidated and interpreted Warfighter/Operator assessments of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) technologies while other agencies, Joint Interoperability Test Command (JITC), under DISA, and the National Security Agency (NSA) respectively, developed



2008 OBJECTIVES

1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE

2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS

3. ENHANCE CROSS-DOMAIN AND MULTIPLE SECURITY LEVEL INFORMATION EXCHANGE TOOLS

4. ENHANCE INTEGRATED LOGISTICS PLANNING TOOLS

5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY

CWID demonstrations support the Network Centric Warfare construct, leveraging advantages of emerging technology.

■

assessments for Technical/Interoperability and Information Assurance. Warfighter inputs were gathered as technologies were pressed into service during the scripted scenario. Collective comments from the operations floor, interpreted for each technology, provided focused insight into user interface, operational utility, and integration issues.

USEUCOM was host combatant commander for CWID 2006-2008. Headquartered in Stuttgart, Germany, the command brought a native coalition emphasis. The scenario described notional coalition task force operations applicable in any global crisis with scripted terrorist and natural disaster events for North American Aerospace Defense Command-U.S. Northern Command (NORAD-USNORTHCOM) Homeland Security and Homeland Defense (HS/HD) coalition of first response partners. CWID supported NORAD-USNORTHCOM, providing investigation of systems integration and interoperability solutions among interagency partners including the Department of Homeland Security and Public Safety and Emergency Preparedness Canada.

CWID demonstrations support the overall Network Centric Warfare (NCW) construct, leveraging advantages of emerging technology. During the demonstration execution phase, trials were conducted over, or connected to, a global network that supports military and coalition operations while providing infrastructure for Defense Support to Civil Authorities (DSCA). The CWID Joint Management Office (JMO), under Defense Information Systems Agency (DISA) direction, coordinated, engineered, and supervised the network backbone(s), information domains and the worldwide venue.

U.S. Joint Forces Command (USJFCOM), Norfolk, VA, provided oversight of planning and execution, targeting information technologies that could be moved into operational use in the short term by focusing attention through CWID assessment results. Strategies aimed at responsibly bringing technology solutions to the Service acquisition community are a yearly effort.

DISA, Arlington, VA, managed day-to-day program operations, directed execution and established a simulated operational network for the demonstration. The network enabled classified information to accommodate information flow for the full spectrum of coalition military operations and unclassified interface for disaster response.

NORAD-USNORTHCOM, Peterson Air Force Base, CO., managed the HS/HD portion of the demonstration. The command used CWID to prove emerging technology application through the full range of first responders, from the Department of Homeland Security (DHS) to municipal police departments.

CWID Leadership

THE CHAIRMAN, JOINT CHIEFS OF STAFF mandates CWID, delegating oversight to U.S. JOINT FORCES COMMAND (USJFCOM) CWID director and soliciting support from U.S. combatant commanders, Services and agencies and multinational participants.

USJFCOM provides oversight for CWID as chairman of the SMG, voting only in case of a tiebreaker. In coordination with the host combatant commander, USJFCOM gathers, consolidates, and formulates overarching objectives that guide industry engagement through the Federal Business Opportunities announcement. Working closely with Services, international coalitions, NATO, and government agencies, they provide the vision for long-term planning. USJFCOM unites interoperability trial sponsors and mentors to highlight promising technology candidates for post-execution transition decisions.

THE DEFENSE INFORMATION SYSTEMS AGENCY (DISA) CWID JOINT MANAGEMENT OFFICE (JMO) manages daily operations, plans, and executes CWID. DISA creates and maintains the demonstration network and information architecture enabling controlled and protected communications as prescribed by operational requirements and national security policies.

THE CWID HOST COMBATANT COMMANDER, generally serving for two consecutive years at a time, provides overarching warfighter guidance, planning and execution leadership; assists in prioritizing CWID objectives; and creates a simulated operational environment with a multinational task force staff (as required).

North American Aerospace Defense Command - U.S. Northern Command (NORADUSNORTHCOM) is the lead for Homeland Security/Homeland Defense play.

THE MILITARY SERVICES provide CWID planning and execution leadership, propose and/or sponsor trials, encourage active participation in selected trials, and designate a service execution site.

COMBATANT COMMANDERS provide, monitor, and update coalition C4ISR interoperability issues and capability gaps.

COALITION PARTNERS provide input through the entire planning process and may submit coalition C4ISR interoperability issues and challenges to the Joint Staff/J-6 for consideration in establishing the CWID objectives. The Coalition Coordination Group (CCG) is encouraged to propose and/or sponsor Interoperability Trial (ITs) in response to the CWID mirror message and to participate in the SMG IT and demonstration selection process.

USEUCOM, Kelley Barracks, Stuttgart, Germany, was host site for CWID 2008. Other U.S. operational sites included: HS/HD at NORAD-USNORTHCOM, Peterson Air Force Base, CO; U.S. Army, U.S. Marine Corps and National Guard Bureau at Naval Surface Warfare Center, Dahlgren Division (NSWCDD), Dahlgren,VA; U.S. Navy at Space and Naval Warfare Systems Command (SPAWAR), San Diego, CA; U.S. Air Force at Electronic Systems Center (ESC), Hanscom AFB, MA; and Warfighter Capability Demonstration Center (WarCap), Pentagon.

The scenario was a notional coalition task force operation applicable in any global crisis with scripted terrorist and natural disaster events for NORAD-USNORTHCOM's HS/HD coalition of first response partners. CWID supported NORAD-USNORTHCOM, providing investigation of systems integration and interoperability solutions among interagency partners including DHS and Public Safety and Emergency Preparedness Canada.

The global network included Canada, New Zealand, United Kingdom, NATO and Partnership for Peace nations with independent trials and network demonstration sites.

The global network included Canada, New Zealand, United Kingdom, NATO and Partnership for Peace nations with independent trials and network demonstration sites. There were more than 20 multinational participants around the world.

Yearly process improvements facilitate development of strategies aimed at responsibly bringing technology solutions to the DoD Acquisition, Technology and Logistics (AT&L) community for consideration. CWID management is committed to information sharing solutions that are built on a net-centic, enterprise-driven, secure, scaleable, and bandwidth-sensitive foundation.

DEMONSTRATION NETWORK LOCATIONS

Operational Reports

U.S. EUROPEAN COMMAND (USEUCOM), KELLEY BARRACKS, STUTTGART, GERMANY

As lead combatant commander and Coalition Task Force (CTF) Commander in the scenario, USEUCOM engaged a spectrum of players including senior CTF warfighters from Germany, NATO, New Zealand and United Kingdom. Other uniformed staff originated from: U.S. Army Reserve, Columbia, SC; U.S. Army from Colorado Springs, CO; U.S. Navy Reserve (USEUCOM Detachment 0208) from Atlanta, GA; and U.S. Air Force from Ft. Meade, MD. These warfighters played a significant role providing coalition perspective in the CWID Technology assessment.

USEUCOM ran 16 trials from their command network hub, discovering four technologies with potential to solve communications interoperability issues with NATO forces. In light of this, USEUCOM pursued more scenario events with the United Kingdom and NATO Response Force (NRF) command staff in Lillehammer, Norway.

Technologies favored in the command coalition environment were centered on ability to share information and collaborate within ad hoc communities of interest (COIs) at lower classifications while still maintaining core content and output control.

One hardware solution addressed encryption at a higher security level for mobile computing, specifically tactical situations where information is most vulnerable to cature by enemy forces.

...warfighters played a significant role providing coalition perspective in the CWID Technology assessment.

NORTH AMERICAN AEROSPACE DEFENSE COMMAND – U.S. NORTHERN COMMAND (NORAD-USNORTHCOM), PETERSON AIR FORCE BASE, CO

The NORAD-USNORTHCOM site is the lead for Homeland Security and Homeland Defense (HS/HD) activities in CWID. The command coordinates HS/HD activities among participating sites and hosts two operations centers (NORAD and USNORTHCOM Battle Staff and National Guard Bureau Joint Operations Center) to exercise and assess participating trial capabilities.

The site supported assessment of 16 trials. Within the USNORTHCOM site, the U.S. Coast Guard conducted two virtual trials assessed by their Battle Staff Liaison Officer. Five trials were of interest to site visitors and participants. These trials supported automating commander update briefings, incident

management, information sharing and agency coordination, deployed staff reachback to home headquarters workstations, and data-at-rest security.

During the CWID demonstration, USNORTHCOM's operations staff played on a limited scale with a broad spectrum of participants from local to state (state government and National Guard) to Federal (DoD and non-DoD) and bi-nationally with Public Safety Canada and Canada Command to address cross-border incident support and information sharing.

The Battle Staff and National Guard Bureau (NGB) Joint Operations Center (JOC) used real-world flooding in the Midwest for free play, employing trials to gather and disseminate information for the twice-daily commander situational awareness briefings. Additionally, Battle Staff members encouraged trial operators at each of the CWID HS/HD sites to brief how they were using trial capabilities. This gave the entire distributed community an opportunity to see what value trials were bringing to operations.

The USNORTHCOM site was supported by: 207th Army Liaison Team (U.S. Army Reserve Command); Colorado Army and Air National Guards; Naval Surface Warfare Center (NSWC) remote facility, Crane, IN; NORAD and USNORTHCOM Standing Joint Force Headquarters-North; and Battle Staff Liaison Officers from Canada Command, Federal Emergency Management Agency (FEMA) Region VIII, and U.S. Coast Guard Reserve.

State Emergency Operations Centers Participate in the CWID Scenario for Technology Trials

CALIFORNIA: The San Diego State University Visualization Center, San Diego, CA, is the hub of the university's homeland security and first-response outreach efforts. The center offers a dynamic capability for reconfiguring display and analysis of large data sets on as many as eight different display screens in a user-defineable command and control center setting.

High-speed optical connections enable the center to transmit and receive large volumes of data while working collaboratively with other command and control centers and researchers in the field. Internet, experimental optical and special high-performance wireless networks all converge in the Visualization Center to provide extraordinary connectivity for the university and the community.

The center works directly with the first responder community, frequently for exercises, real-world events and planning.

During CWID 2008, the center functioned as both state of California and city of San Diego level Emergency Operations Centers (EOCs).

VIRGINIA: The Virginia Department of Emergency Management (VDEM) Operations Division operates and maintains the 24/7 Virginia Emergency Operations Center (VEOC) located on the grounds of Virginia State Police Headquarters, Richmond. The VEOC staff is equipped and ready to provide assistance as required or requested throughout the Commonwealth.

Daily operations include Search and Rescue coordination, Hazardous Material Response coordination, and weather monitoring.

The Virginia Emergency Response Team (VERT) includes trained and ready experts from state agencies, voluntary organizations and private partners to staff the VEOC, coordinate response efforts and provide situation reports on existing conditions and requirements.

In addition to operational direction and control at the VEOC, disaster response activities include disaster resource prioritization, information gathering and situational/damage assessment, mission assignment and tracking, resource management, legislative liaison, community outreach, public affairs and executive coordination.

WEST VIRGINIA: The Office of the Cabinet Secretary for Military Affairs and Public Safety (WV-DMAPS), Charleston, WV, is the overall responsible agency for coordinating, facilitating and synchronizing efforts to support the state during natural disasters, National Special Security Events, exercises and domestic activities.

Organizations serving in any event are typically driven by the nature, complexity, and scale of the event itself. For planning purposes, HS/HD believes that a significant event in the Metro DC area could force a migration of personnel with vehicles through West Virginia.

It is in that scope that WV participated in CWID. During CWID 08, all 55 counties of West Virginia were involved. The approximate 1/3 counties directly involved with a migration from the DC area were on full activation. Another 1/3 of WV counties would be "touched" by such an event. There were exercises for some of these counties and their respective OESs were stood up.

The last 1/3 of the counties would likely not be involved in such a migration, but could be asked to provide support to the other counties. For this reason, they were simply on alert.

Involved in CWID 08 were WV-DMAPS, WV-DHSEM, WV-National Guard, WV-Department of Transportation, WV-Department of Health and Human Services, WV-State Police, and a host of local and county first responders and Homeland Security personnel.

Further, WV-DMAPS serves as the "State" command and control element for WV Division of Homeland Security and Emergency Management (DHSEM) and WV National Guard.

The WV National Guard coordinates efforts with WV-DHSEM, National Guard Bureau, and other Federal agencies. The 35th Civil Support Team Tactical Operations Center deploys to a domestic CBRNE incident site in support of civil authorities by identifying CBRNE measures, and assisting with requests for additional support. The unit is comprised of 22 Army and Air National Guard personnel.

The Tactical Operations Center is a van equipped with cell phone to radio connection; Inmarsat B, commercial Ku Band, and UHF SATCOM; 800 MHz radio interlink, NIPRNET/SIPRNET/internet access and land line phones.

The WV-NG also hosts three mobile communications vans that are deployed via the J6 staff. These vans host a range of communications assets similar to the 35th CST and is C130 transportable. These J6 mobile communications vehicles are staffed and self contained.

The Battle Staff and NGB JOC used on-going flooding in the Midwest for free play.

NAVAL SURFACE WARFARE CENTER, DAHLGREN DIVISION (NSWCDD), DAHLGREN, VA

NSWC Dahlgren is the U.S. Marine Corps and U.S. Army site, hosting the Combined Forces Land Component Commander (CFLCC) for the CTF scenario. Augmenting scenario reality for the on-site component commander were two tactical elements, a U.S. Marine Corps Command Operations Center (COC), playing on the CTF network, and a U.S. Coast Guard mobile command post, actually a trial in the demonstration, on the HS/HD network. Tactical units in the scenario: 1st Marine Expeditionary Brigade (MEB); 31st Marine Expeditionary Unit (MEU); 15th MEU; NGB; Naval Sea System Command (NAVSEA) Sea Trials unit;

and US Coast Guard (USCG) participated here.

Dahlgren hosted 31 Interoperability Trials (ITs) on the CTF and HS/HD networks in seven separate operational centers. Eighteen trials participated on CTF, 13 on HS/HD and two of 31 trials demonstrated on both domains. Tactical units represented in the scenario and on the assessing warfighter staff were 1st Marine Expeditionary Brigade (MEB), 31st Marine Expeditionary Unit (MEU), and 15th MEU. Other staff represented in operational centers were NGB, NAVSEA Sea Trials unit, and USCG.

Warfighters at Dahlgren found 5 trials of particular interest, ranging from global situational awareness technologies and mission support systems to automated network filtering and load control.

NAVSEA Naval Reserve unit and Guided Missile Destroyer DDG 1000 operational center employed U.S. standard fires systems, i.e., Naval Fires Control System (NFCS), Joint Automated Deep Operations Coordination System (JADOCS), and Advanced Field Artillery Tactical Data System (AFATDS), to execute calls for fire from Dahlgren using Global Command and Control System (GCCS) threads. Systems across the CFBLNet executed target missions involving the U.S. systems and the United Kingdom-Joint Effects Tactical Targeting System (UK-JETTS).

This year Dahlgren hosted Joint Users Interoperability Communications Exercise (JUICE) 2008 as Marine Forces (MARFOR) concurrent with CWID demonstration.

Vice Admiral Nancy Brown, Joint Staff Director for Command, Control, Communications and Computer Systems, listens to a technology briefing from an operator at the U.S. Northern Command CWID demonstration site.

Trident Warrior, the U.S. Navy's major annual operational FORCEnet Sea Trial event, will take selected CWID trials into a more focused operational environment for further evaluation.

■

SPACE AND NAVAL WARFARE SYSTEMS COMMAND (SPAWAR), SAN DIEGO, CA

SPAWAR hosted the Combined Forces Maritime Component Commander (CFMCC) and successfully integrated a robust HS/HD presence, significant because the environment employed cross-domain solutions. Operators on the classified CTF network collaborated with unclassified operators on the HS/HD side, to include the San Diego Police Department (SDPD) and demonstration Emergency Operations Centers (EOCs) at San Diego State University (SDSU) and at SPAWAR.

The U.S. Navy site assessed 21 trials, 15 on the CTF network and six on HS/HD. Three information technologies operated on both domains. Operators favored eight technologies during scenario play, ranging from secure data access and automatically managed network traffic to global coalition maritime domain awareness collaboration capabilities. One system of note on the HS/HD network allowed the SDPD to access common communication and collaboration from a full range of standard police department devices to high-tech military satellite capabilities.

Naval warfighters originated from: U.S Navy Reserve programs; the German, Italian and New Zealand navies on command staff; Command, Naval Region Southwest Active Duty Navy personnel; California Air National Guard, a U.S. Air Force technician working HS/HD; and the San Diego Police Department. Exchange among U.S. and coalition warfighters and HS/HD first responders is a continuing key to success of SPAWAR's CWID.

Guard and Reserve personnel bring military civilian skill sets and training and experience to the effort. SPAWAR warfighters continue to provide valued assessments of technologies before they reach formal acquisition. The entire team made unbiased comments that identified which technologies were ready to move on to operational testing or fielding, and noted technologies that needed more developmental work before being demonstrated again. Trident Warrior, the U.S. Navy's major annual operational FORCEnet Sea Trial event, will take selected CWID trials into a more focused operational environment for further evaluation.

SAN DIEGO STATE UNIVERSITY PARTICIPATION

A tiered-level EOC was significant this year, demonstrating command, control and communications through a chain-of-command, spread over four locations, with members from four very different organizations.

SDSU Visualization Lab role players staffed and functioned as the state and city level EOC, providing support and oversight to an on-site EOC and first responders located at SPAWAR. Back for the third year, the SDPD provided an officer for on-site EOC Watchstander and liaison.

ELECTRONIC SYSTEMS CENTER (ESC), HANSCOM AIR FORCE BASE, MA

ESC is the sole Air Force site in CWID. The site hosts the Combined Forces Air Component Commander (CFACC) and operates a small-scale Combined Air Operations Center (CAOC) with the primary mission of publishing the daily Air Tasking Order/Air Control Order (ATO/ACO) and providing the simulated air campaign picture for the CWID scenario.

ESC hosted coalition partners from three countries: Canadian Forces sent five participants for trial management; Denmark provided four participants for core service support for ATO/ACO conversion; New Zealand dedicated one warfighter as lead mission planner. Nineteen U.S. warfighters supported operations: four Active Duty Air Force; nine Air National Guard members from Massachusetts and Arizona; and six Air Force Reserve members from ESC.

A total of 22 trials participated at ESC. Sixteen participated in the CTF scenario, while six trials participated in the HS/HD scenario. A number of trials earned high marks from warfighters. One trial enabled migration of Air Force Weather Weapon System forecasting and product-tailoring competencies to a single common-user-interaction capability. This improved the ability to gather, process, analyze, and produce environmental (i.e., terrestrial, space) data and products. With great success, ite managers combined a number of trials to showcase interoperability and spur future collaboration for additional capabilities.

Concurrent with CWID 2008 Execution, ESC participated in the CyberSpace Symposium II, Marlborough, MA, with an information booth. Several symposium attendees visited the ESC CWID site and expressed interest in CWID 2009 participation.

The Johns Hopkins University Applied Physics Lab partnered with an interoperability trial to collect a human interface and system operation data. CAOC Performance Assessment System (CPAS) gathered physiological data from the Senior Offensive Duty Officer (SODO). Using CPAS technology, "seeing machines" traced eye movements and thought-sensing technology collected data, providing a stored, correlated, and retrievable history of events during real-time CAOC operations -- to answer the question "What happened?" as a training and system optimization tool.

A tiered-level EOC was significant at SPAWAR this year, demonstrating the capability to command, control and communicate through a chain-of-command, spread over four locations, with members from four very different organizations.

■

The Canadian approach for CWID is to combine activities of the Department of National Defence and the Department of Public Safety, as they relate to HS/HD.

CANADIAN FORCES EXPERIMENTATION CENTER, SHIRLEY'S BAY, OTTAWA, ONTARIO, CANADA

August 2007, the Assistant Deputy Minister (ADM) for Information Management (IM) assumed responsibility for CWID. The Director General Information Management Organization (DGIM)/J6 Coordination identifies IM capability deficiencies, selecting information technologies with the potential to address identified gaps, scenario development, training, execution coordination, public relations, the visitor program, trial assessment and after action reports.

Canadian Forces Experimentation Centre (CFEC), previously responsible for CWID, retained responsibilities of hosting CWID and providing support to include: provision of labs and lab support, CFBLNet administration, network and physical security, and demonstration administrative support.

The Canadian approach for CWID is to combine activities of the Department of National Defence and the Department of Public Safety, as they relate to HS/HD.

Canada operated a main site at Shirleys Bay, near Ottawa, with a satellite site in Valcartier, near Quebec City. Canadian liaison teams were provided to four other CWID sites: ESC, Hanscom AFB; Lillehammer Norway; NSWC Dahlgren; and NORAD-USNORTHCOM.

Since CWID 2008 was a transition year for ADM (IM), Canada hosted two and participated in ten Interoperability Trials (IT). The two Canadian sponsored trials performed extremely well with effective training packages, linked to IT capabilities and functions, which were in turn linked to the Master Scenario Event List (MSEL) and the resulting Assessment Plan.

Canadian role players came from the Canadian Government Operations Centre, the Air Force, the Joint Information and Intelligence Fusion Centre Detachment, and Canada Command.

HEADQUARTERS JOINT FORCES NEW ZEALAND (HQ JFNZ), TRENTHAM, NEW ZEALAND

New Zealand Defense Force (NZDF) participation in CWID activities focuses upon exposing the operational community (operators) to allied developments in the interoperability of Command and Control (C2) systems technology and assessing applicability to the NZDF. CWID also provides a vehicle to identify concepts to develop the Network Enabled Capability Roadmap and validate identified capability options and operational concepts.

CDR Rodger Ward, J6 of Joint Forces, explained, "Our warfighters examined a product based on Microsoft SharePoint collaboration software that provided a portal through which military units share common information via a single access point on the 'save once use many principle,' and a Java client that would allow units in the field easy access to their HQ's over-arching C2 system and COP [Common Operational Picture] via PDA's or laptops.

"We also tested an information sharing product based on security protocols that would allow defence forces and other government agencies to share restricted intelligence information when previously set conditions are met. These types of technologies reduce requirements for multiple secure networks by managing access to content through logons and rules -- a better way of doing business."

The NZDF established two CWID sites for participation, the primary at HQ JFNZ, which focused on improving situational awareness of operations by demonstrating an improved briefing and visualisation suite for the operational watch centre. The secondary site located within the recently formed Integrated Mission Support Squadron (IMSS), Royal New Zealand Air Force (RNZAF) Base Auckland, acted as an AOC, which included demonstration of a fully integrated briefing and collaboration suite.

Fifty percent of trials participating were selected to migrate to New Zealand Service within six month

HQ JFNZ officers managed maritime air current operations, employing a scenario that migrated though the phases of a three-block war matrix. Warfighters from all contributing nation's operated technologies, participating in real-time to demonstrate information sharing over a classified wide area network. The RNZAF CWID Site Manager and lead Air Planner, SQN-LDR Glenn Gowthorpe believes that CWID provided an excellent opportunity to focus warfighters, CIS engineers and network staff on the planning, setup and execution of complex hardware and software systems with the prime goal of increasing operational support and interoperability.

...CWID provided an excellent opportunity to focus warfighters, ... engineers and network staff on the planning, setup and execution of complex hardware and software systems with the prime goal of increasing operational support and interoperability.

■

Potential capability gap solutions, risk reduction activity supporting currently funded projects, and innovation and experimentation support are direct benefits [of CWID].

DEFENSE SCIENCE AND TECHNOLOGY LABORATORY (DSTL), PORTSDOWN WEST, UNITED KINGDOM

The United Kingdom (UK) is committed to meaningful participation in CWID to improve interoperability in a coalition context. Involvement in CWID is sponsored from within the UK Ministry of Defense (MOD) by the Capability Manager (Information Superiority). Director Equipment Capability (Command, Control and Information Infrastructure) delivers the program. The CWID UK concept focused on a Network Enabled Capability (NEC) and examining and identifying solutions to the gaps that have emerged from current operations.

CWID directly benefits industry, the MOD, and wider government by providing a vehicle to demonstrate current and emerging technology, balanced by operational requirement from UK forces. Potential capability gap solutions, risk reduction activity supporting currently funded projects, and innovation and experimentation support are direct benefits. CWID also provides both the UK MOD and industry with technical and financial leverage, training and process opportunities, and partnership development.

In 2008, the UK focused on five broad areas of interest: resilient information infrastructure; Command and Control (C2) and shared situational awareness; end-to-end Intelligence, Surveillance, Targeting, Acquisition and Reconnaissance (ISTAR) processes; logistical information; and information assurance. The demonstration was conducted on a secure, web-based, open architecture using internet protocol (IP). The network reflected current deployments, while demonstrating what was technically feasible in the future

UK CWID demonstration managers

stressed operational context, successfully mapping the trial assessment environment to real-world coalition-force operations. During the operational scenario, managers demonstrated Multi-lateral Interoperability Program (MIP) and introduced UK Coalition Secure Management Operation System (COSMOS), a version of technology demonstrated in U.S. CWID 2006 and 2007. CWID 2008 successfully demonstrated UK-US interoperability through air command and control, ISR and targeting, and shared situational awareness trials.

UK MOD provided in excess of 80 military staff to support CWID trial evaluation at UK sites. One officer from the Land Information Assurance Group was a NATO liaison at Camp Joestadsmoen, Lillehammer, Norway. A UK Officer supported the WARCAP, demonstrating the operational context of CWID UK. U.S. DoD supported UK efforts by providing three staff throughout CWID Execution. The UK assessed 32 trials, demonstrating the ability to operate on a single networked infrastructure and running a common secure architecture that ensured the integrity of all systems. Additionally, six U.S. sponsored Interoperability Trials (ITs) participated in the UK for network interaction with U.S. sites.

UK CWID remained a high profile event with over 700 visitors to the UK site, including senior U.S. DoD personnel. UK CWID managers will continue to stress operational context, and, in the process, press for a coalition environment that reflects real-world operations.

NATO AT CAMP JORSTADMOEN COMMAND AND CONTROL TRAINING CENTER, LILLEHAMMER, NORWAY

NATO CWID is an annual NATO Military Committee (MC) directed event designed to bring about continuous improvement in interoperability for the Alliance. This event was established in 2004 by the NATO MC as a key tool to affect transformation within the Alliance. For 2008, the NATO CWID programme focused on testing, assessing and ultimately improving the interoperability of multi-national C4I systems, with particular emphasis on those normally deployed within a NATO Response Force (NRF) or a Deployed Joint Task Force (DJTF).

In addition to bilateral technical testing, NATO CWID provides a venue to conduct technical testing of fielded, developmental and experimental systems in the context of a coalition scenario. The operational commitments for the NRFs tested in 2008 commence in 2010. Interoperability issues that are identified as a result of trials conducted in CWID can be addressed and resolved prior to Steadfast Cathode 2009.

In addition to seven NATO agencies and organizations involved, 16 nations participated from Lillehammer. Three additional nations were present as observers. NATO CWID tested NRF C4I systems from: Air, Maritime, Land, and Special Operations.

In CWID, the land component and special operations component tested interoperability between Command and Control (C2) systems that use Multilateral Interoperability Program (MIP), NATO Friendly Force Identification (NFFI) and Allied Data Publication (number) 3 (ADatP-3) formats.

The Maritime Component employed multiple NATO task forces including a carrier battle group with associated surface and subsurface combat units, amphibious forces, naval MCM units and auxiliary support vessels. A force so large would not normally deploy as an NRF, however, it was structured for testing among a number of maritime command and control systems.

The Air Component structure allowed testing between the fielded ICC C4I system and the experimental system, ACCS.

Assessments conducted at NATO CWID are important to the program in general and to the operational commander specifically. However, of greater importance, are those systems found to have interoperability shortfalls while being run at NATO CWID. A significant contributions of NATO CWID is on-site problem solving by NATO and national system engineers.

NATO and its coalition partners are more interoperable than ever. Resolution of interoperability challenges thrives with the active involvement of Nations and all levels of the NATO Command structure under a coordinated program.

NATO CWID provides a unique opportunity for interoperability testing, assessment, and demonstration as well as invaluable face-to-face human collaboration. Hence, NATO CWID is highly valued by NATO and nations for its proven track record of identifying and resolving interoperability issues.

PARTICIPATING NATO NATIONS:

Canada
Czech Republic
Denmark
Germany
France
Italy
Norway
Poland
Romania
Spain
Turkey
United Kingdom
United States

NON NATO NATIONS

Finland
New Zealand
Sweden

WARFIGHTER CAPABILITY DEMONSTRATION CENTER (WARCAP), PENTAGON

WarCap supported CWID for the second year, providing senior leaders in the National Capitol Region a local vantage point from which to observe the worldwide demonstration. The WarCap is a unique interactive theater linked through the CFBLNet to all CWID U.S. operational sites, plus Portsdown West, UK.

The network is an on-going protected venue for coalition interoperability testing that is the backbone for the CWID demonstration every year.

Coalition partners demonstrating information technologies during this year's WarCap sessions included officers on scenario command staffs from the United Kingdom, Denmark, Canada, Italy, and Germany.




FROM U.S. JOINT FORCES COMMAND

Most Promising Technologies, 2008

The interoperability trials (ITs) below successfully achieved stated objectives and favorably impressed warfighters/operators and technical assessors as relevant solutions for meeting combatant command and service capability gaps.

Based on the Quicklook survey* responses captured during the execution phase from participating warfighters/operators, Network Operating Working Group (NOWG), Systems Engineering and Integration Working Group (SEIWG) and Site Managers/ Engineers, the highlighted trials were recommended to the Senior Management Group (SMG) as the CWID Most Promising Technologies for this year's demonstration. CWID 2008 assessed 41 trials on three operational network domains.

NOTE: Trials are listed in order of "Quicklook" survey results in each of vendor funded and government funded categories. *Quicklook" represents results from SMG-approved surveys completed by warfighters and assessors during the demonstration. It reflects immediate detailed impressions of information technologies in the CWID operational environment. Individual detailed reports in the unabridged Final Report (on CD and online at www.cwid.js.mil) include in-depth analysis, extensive assessments of technical solutions demonstrated during CWID execution.

CWID 2008 Most Promising Technologies, Vendor Funded

Trial No.	Title (Acronym)	Sponsor	Developer	Page
5.73	**VirtualAgility OPS Center (VOC)**	Canada	IBM	44
	VirtualAgility OPS Center is a browser-based software solution that enables interoperability and coordination within and among agencies to organize, plan, track and share operational activities. This open-standards technology connects incompatible systems, preserves the integrity of proprietary databases and streamlines personnel identification, location, collaboration and communications.			
1.15	**Datatek IPv4-IPv6 Transformer**	US Army	Datatek Applications, Inc.	26
	The IPv4-IPv6 Transformer instantly converts IPv4-only legacy systems into dual-stack IPv4/IPv6 systems, to enable IPv6 messaging, while preserving IPv4 pass-through mode.			
5.34	**Poliwall with HIPPIE Security Appliance**	DISA	TechGuard Security LLC	42
	PoliWall's HIPPIE Appliance filters block network traffic from adversary nations and gives U.S. and coalition partners higher priority to network assets. Policies can be quickly configured using a simple and intuitive world-map based interface.			
5.65	**Security Information Management for Enclave Networks (SIMEN)**	US Air Force	The MITRE Corp	44
	SIMEN incorporates algorithms and protocols for the distributed collection and transport of IA events to a central location. SIMEN uses protocols and adaptive algorithms to dynamically respond to evolving threat environments, respect bandwidth constraints, prioritize events, and minimize fluctuating event volumes.			

5.06	**Common Information Centric Security (SecureD®)**	OSD	Techsoft Inc.	40
	SecureD® provides data at rest encryption. Sponsored by the U.S. office of the Secretary of Defense, SecureD® is the product of a joint US-Norwegian project and has earned Common Criteria EAL4+ and FIPS 140-02 Level 3 certifications			
1.62	**RIOS Incident Site Communications Capability (RISCC)**	USNORTHCOM	SyTech Corp.	32
	RISCC provides both local and wide area interoperability with enhanced command and control features: remote radio control; logged RIOS chat; remote site operations; incident recording; playback; and reporting. The system operates with civilian and military communications devices including radios, phones and computer and with legacy devices, connecting civilian agencies, first responders and military units.			

CWID 2008 Most Promising Technologies, Government Funded

Trial No.	Title (Acronym)	Sponsor	Developer	Page
2.84*	**Smart Data Flow (SDF or CCER-8)**	DISA	Referentia Systems Incorporated	39
	SDF is an Office of Naval Research (ONR) and U.S. Pacific Command initiative that addresses DISA's CENTRIXS Cross Enclave Requirement for managing services on converged networks in the enterprise coalition environment. SDF provides an intelligent network management solution for controlling and configuring network devices in real-time. This software application's extensive visualization capabilities improve network situational awareness and allow less seasoned operators to manage networks with reduced risk of error.			
2.82*	**Proximity-Sensitive Session-Support Services (PS4 or CCER-6)**	DISA	NETCON Solutions	38
	PS4 addresses converging networks, leverages existing infrastructure and provides transparent, discretely separated Communities of Interest (COI) without user interaction, using existing transport. The technology supports central management by integrating with existing JTF-GNO central management and provides local and global COI separation by enabling COI boundaries by central administrators and varying access controls. PS4 builds dynamic, type 2, VPN tunnels and establishes end-to-end connectivity without relying on VPN concentrators.			

1.22	**Army Future Combat Systems Joint Interagency Multinational Interoperability (FCS JIMI)**	US Army	US Army	27
	FCS is an Army Acquisition Category (ACAT) I "D" (for "Defense Acquisition Board (DAB)" program. The FCS Brigade Combat Team (BCT) Program is the Army's primary transformation and modernization effort. It consists of a family of networked manned/unmanned systems including: unmanned aerial vehicles, unmanned ground vehicles, and unattended sensors/munitions. This system will equip and transform the Army Modular Force.			
2.27*	**Compartmented High Assurance Information Network (CHAIN or CCER-3)**	DISA	Raytheon	36
	CHAIN provides a framework for information sharing. Provides a windows-based solution for secure coalition interoperability, a Microsoft Windows-centric SOA (Service Oriented Architecture) for highly scalable interoperability with non-Windows platforms, and a CENTRIXS Cross-Enclave Requirement. Provides email, collaboration, web access, text chat, file sharing, and compartmented voice. Additionally, it provides information security, encryption, digital signatures, and content scanning. It satisfies fewer infrastructures, requires fewer people, allows better communication and needs less training.			
2.83*	**Agile Coalition Environment (ACE or CCER-7)**	DISA	Referentia Systems Incorporated	39
	ACE is a National Security Agency (NSA) supported U.S. Pacific Command initiative designed to address DISA's Combined Enterprise Regional Information Exchange System (CENTRIXS) Cross Enclave Requirement (CCER) for Collapsed Networks. The ACE architecture provides a foundation for secure and agile enclave instantiation and cross domain access.			
2.28*	**Secure Information Sharing Architecture (SISA or CCER-4)**	DISA	TKC Communications	36
	SISA provides coalition warfighters a commercial off-the-shelf (COTS) solution for secure information sharing. SISA is created to house multiple communities of Interest (COI's) in a single consolidated environment. The tenets of the architecture include access protection, management and controls for authenticated access to networks, client, and server endpoints, content protection, collaboration services with persistent protection against inadvertent or malicious disclosure of files, documents, and e-mails.			
2.29*	**Federated Identity Management System (FIdM or CCER-5)**	DISA	Bearing Point	37
	FIdM shares information across Communities of Interest (COI) effectively and securely. The solution integrates various commercially available Identity and Access Management products to provide cross-enclave Access Control. FIdM addresses the data Access Control capability for Combined Enterprise Regional Information Exchange System (CENTRIXS) Cross Enclave Requirement (CCER).			
2.46	**Information Integration Dashboard for Mission Planning Support (IID)**	Canada	Canada	37
	IID is a middleware based network centric environment for information/data integration. This decision support system is essentially a multi-layer IT platform that provides a plethora of services such as data and service integration, monitoring, analysis and process optimization. The platform uses advanced display mechanisms to render structured information and provide navigational representation to drill down into details.			

***TRIAL SERIES NOTE:** The Combined Enterprise Regional Information Exchange System (CENTRIXS) Cross Enclave Requirement (CCER) goal is convergence of multiple separate coalition networks into a single environment at the secret-releaseabe domain. The system is capable of establishing multiple Communities of Interest (COIs) within the secret-releaseable environment. CCER enables warfighters to rapidly and seamlessly share information within and between COIs. The CCER CWID trials, DISA sponsored, are an effort to view and assess mature products and technologies in an operational environment that have the potential to meet set requirements.

NOTES

CWID 2008 OBJECTIVES

Objectives Address Capability Gaps

CWID 2008 charged that information sharing solutions should be built on a foundation that is net-centric, secure, scalable, and bandwidth sensitive.

CWID 2008 objectives are focused to reflect the following recurring themes: investigating emerging and relevant technologies; demonstrating solutions for combatant command theater capability gaps and challenges; enhancing multi-service, multinational, and interagency cooperation and communication.

Objectives are supported by sub-objectives referencing U.S. and coalition capability gaps.

■

Objectives are linked to the Joint Battle Management Command and Control Roadmap and Joint Mission Threads.

OBJECTIVE
1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE

Enhance leadership's capability to command, control and coordinate across joint & coalition forces, government agencies, non-governmental organizations (NGOs) and first responders.

SUB OBJECTIVES:

- Demonstrate cohesive command and control (C2) linkages between military, government agencies and coalition partners
- Demonstrate enhanced interoperability for NATO Response Force C2
- Demonstrate open & secure mobile C2 capabilities between communities of interest (COIs),
- Demonstrate communication tools that streamline decision-making and integrate with existing systems or that present entirely new solutions
- Demonstrate communication tools that share Chemical Biological Radiological Nuclear Explosive (CBRNE) contingency information with first responders & emergency services
- Demonstrate improved general Identification and Blue Force tracking capabilities
- Demonstrate counter insurgency Indications and Warning tools
- Demonstrate targeting tools for non-lethal weapons and corresponding Margin of Error (MOE)
- Demonstrate systems to rapidly extend communications in support of Defense Support to Civil Agencies (DSCA) operations
- Demonstrate tools to support neutralization of Improvised Explosive Devices (IEDs)
- Demonstrate expanded integration of opensource tools to open standards Service Oriented Architectures (SOAs)
- Demonstrate tools to support the entire deployment process from requirements identification through force closure, including redeployment and rotational operations

EXPLANATION: Improved C4ISR Architecture will aid coalition, military and civilian authorities to harness the power of their respective information environments to collaboratively execute operations even in a bandwidth-constrained environment.

OBJECTIVE
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS

Provide the capability to share information across multiple networks of potentially different security classifications and caveats. Emphasis should be on passing information to both U.S.-controlled coalition networks such as U.S. Central Command's Combined enterprise Regional Information Exchange System (CENTRIXS) and coalition/ alliance controlled networks such as NATO's Initial Data Transfer System (NIDTS), NATO Mission Wide Area Network (WAN), or releasable to Republic of Korea (RELROK). Data sharing encompasses the need for cross-domain solutions (CDS) and the assurance that information passed through CDS can be utilized by systems within all security enclaves.

SUB OBJECTIVES:

- Demonstrate multi-level security & multi-domain applications that promote information sharing with planned and unanticipated mission partners,
- Demonstrate effective network defense applications to protect shared data,
- Demonstrate tools that improve utility, accuracy and timeliness of real time translation for collaboration in specific areas of responsibility (AORs),
- Demonstrate complementary planning tools that support military, local law enforcement, first responders, governmental, non-governmental and coalition planning activities,
- Demonstrate tools to improve Request for Forces (RFF) process,
- Demonstrate tools to improve deployment and visibility of coalition and/or interagency/Private Voluntary Organization (PVO)/NGO forces, and
- Demonstrate use of free-ware and share-ware open

standards capabilities to fully connect civilian and military planners.

EXPLANATION: Coalition operations require an information environment that spans multiple COIs. These COIs may be mobile, fixed or remotely located where the combination of military and/or civil agencies is likely to be affected by limited bandwidth.

OBJECTIVE 3. ENHANCE CROSS DOMAIN AND MULTIPLE SECURITY LEVEL INFORMATION EXCHANGE TOOLS

Provide solutions that improve the commander's ability to share intelligence information products (documents, images, databases, etc.) with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders.

SUB OBJECTIVES:

- Demonstrate data fusion tools that support cross domain information sharing and consolidates multiple sources of information into a single reference source.
- Demonstrate situational awareness tools that disseminate and display time-critical information to tactical forces and first responders to include defense against IEDs.
- Demonstrate visualization and integration tools that can simultaneously manage multiple intelligence, surveillance and reconnaissance inputs.
- Demonstrate capabilities to enhance Maritime Domain Awareness between federal, state and local agencies.

EXPLANATION: Cross domain and multiple security level information exchange represent more than providing a common operational picture at the strategic or major echelon level of command. Exchange tools must be secure, scaleable in scope and functional within the theater bandwidth available at all levels of warfare.

OBJECTIVE 4. ENHANCE INTEGRATED LOGISTICS PLANNING TOOLS

Demonstrate the ability to access, consolidate and display logistics information to include movement, location and status of joint forces, military services, interagency, coalition, NGO, first responders as well as equipment and supplies in near real-time across organizational boundaries.

SUB OBJECTIVES:

- Demonstrate secure abilities to assess and display information regarding the movement, location, and status of Coalition equipment and personnel.
- Demonstrate logistics data access, fusion, and integration among COIs.
- Demonstrate logistic data sharing for medical and health protection services.
- Demonstrate capability to exchange logistic data between government agencies, NGOs and military systems.

EXPLANATION: Within the information environment of coalition, military and non-military operations, the commander must have responsive and effective logistics.

...investigating emerging and relevant technologies; focus on demonstrating solutions for combatant command theater capability gaps and challenges; enhance multi-service, multinational, and interagency cooperation and communication.

OBJECTIVE 5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY

Provide solutions that improve a Combatant Commander's ability to conduct collaborative planning with coalition partners, including joint and coalition forces, government agencies, NGOs and first responders. Focus is on enhanced collaboration and engendering a "need to share" vice a "need to know" culture.

SUB OBJECTIVES:

- Demonstrate data access, fusion and integration among joint forces, international, federal and state agencies and local law enforcement,
- Demonstrate the ability to distribute and track key policy and strategy documents between government agencies.
- Demonstrate tools to improve Information Assurance and posture between government agencies.
- Demonstrate a situational awareness tool that uses advanced visualization technologies capable of integrating existing systems into one common operational picture.
- Demonstrate a Blue Force Tracking (BFT) capability for first responders.
- Demonstrate computer network defense capabilities to support non-military partners,
- Demonstrate computer network capabilities that support collaboration with the Department Homeland Security Emergency Management COI.
- Demonstrate interoperability between international agency systems and DoD, multinational systems to support global disaster relief efforts.

EXPLANATION: Government agency interoperability implies that coalition, military and civilian authorities can harness the power of their respective information environments to collaboratively solve problems and plan operations even in a bandwidth constrained environment.



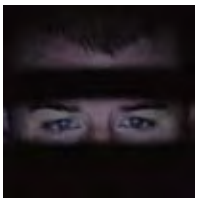
THE ASSESSMENT PROCESS

Three-Pronged Expert Assessment

CWID assessments focus on candidate technologies' ability to provide a short or long-term solution to capability gaps or enhancements to existing solutions. As defined in the CJCSI 6260.01C, the CWID Assessment Working Group (AWG) provides the Coalition/Combatant Commands (COCOMs)/Services/Agencies (C/C/S/A), and other interested parties with an objective warfighter utility, technical/interoperability, and/or Information Assurance (IA) assessment.

THE ASSESSMENT PROCESS

Consisting of three assessment teams, Warfighter Utility, Technical/Interoperability and IA assessment, the AWG's overall goal is to identify potential candidates that provide solutions to capability gaps for Coalition, Joint, and HS/HD operations. During the CWID planning phase, the teams analyse each trial (also known as IT) to determine capabilities, maturity, and other technical factors to approximate the level of effort required for an assessment. This analytical information is then used by the Senior Management Group (SMG) during IT prioritization to allocate assessment resources.



During the CWID planning and execution phases, the assessment teams and IT representatives collaborate to ensure ITs receive meaningful and beneficial assessments. Assessments include inputs from operational users and assessors as well as other participants who may add value through their input. Results are captured during execution and analyzed to determine the degree to which ITs satisfy applicable CWID objectives in the context of the three assessment areas.

The goal of the assessment effort is to identify potential candidates to provide C4I interoperability capabilities or enhancements to Joint, Coalition, and Homeland Security/Homeland Defense operations.

WARFIGHTER/OPERATOR UTILITY ASSESSMENT PROCESS

This assessment focuses on the IT's ability to effectively meet planned technical performance perameters and the scheduled CWID objectives through capability demonstrations.

During CWID execution, warfighters interact with ITs and complete questionnaires. The questionnairs collect relevant data to evaluate each system's utility. In this way, the assessors gauge the individual IT's operational performance, how well it integrates in to the CWID environment and it's overall mission performance.

Inherent in these attributes are Measures of Performance (MOPs) such as information accessibility, accuracy, adaptability, consistency, and relevancy, which are used by operational test agencies to assess warfighter utility during formal testing.

TECHNICAL/INTEROPERABILITY ASSESSMENT PROCESS

The Technical/Interoperability Assessment, performed by JITC, focuses on the IT's ability to exchange usable data with network services or other ITs. During planning, the Technical/Interoperability Assessment Team works with IT representatives to define Information Exchange Requirements (IER) based upon system interfaces, anticipated data exchanges, and mapping to CWID objectives. IERs define information to be exchanged, systems/services involved in the exchange, information necessary, and how the exchanges occur.

During execution, assessors witness exchanges to verify data completeness, timeliness and correctness. Results are documented in a database which is included in the CWID Final Report. Data collected during this assessment may be used to support a CJCS Mandated Joint Interoperability Certification with caveats.

INFORMATION ASSURANCE ASSESSMENT PROCESS

The IA Team performs varying levels of analysis during the CWID planning, execution, and reporting phases. ITs may receive one of three types of IA Assessments: Basic, Conceptual, or Targeted. All ITs connected to the CWID networks during execution received a Basic Assessment; a non-intrusive discovery scan using DoD approved tools.

The Conceptual Assessment was performed on U.S.-sponsored ITs that are virtually connected to U.S. sites. It was intended to familiarize the vendor with information assurance policies and practices while recording and analyzing data against vendor claims. The Targeted Assessment provided analysis of the Conceptual Assessment while using vulnerability analysis tools to substantiate vendor claims.

IA Assessment results may be used by the vendor to improve the system's IA posture and by the sponsor to gauge risks associated with potential procurement of the solution following CWID.

The Assessment Working Group is comprised of three separate analyst teams that provide three different categories of assessments:

- *Warfighter/Operator Utility*
- *Technical/ Interoperability*
- *Information Assurance*

CWID EXECUTION

During execution, AWG members were on-site at USEUCOM, NORAD-USNORTHCOM, NSWC Dahlgren VA, SPAWAR San Diego CA, Hanscom AFB, MA. Additionally, Canada, NATO, New Zealand and United Kingdom provided on-site assessment support to collect data and evaluate trial performance. Of the 41 ITs that participated in CWID 2008, 30 trials received a Warfighter Assessment, 34 received a Technical/Interoperability Assessment and 36 received an Information Assurance Assessment. SEIWG reported results on seven ITs that did not recieve formal Technical/Interoperability assessments.




TWO-PART SCENARIO

The Environment for Technology Trial Assessment

The scenario described notional coalition task force operations applicable in the current environment with terrorist backlash and natural disasters for North American Defense - U.S. Northern Command's (NORAD-USNORTHCOM) Homeland Security and Homeland Defense (HS/HD) component. The simulated operational environment provided context for validation of proposed technology solutions.

COALITION SNAPSHOT, DAY 3

- Nevatah invades Terrizona at dawn to consolidate terrorist foothold; all Coalition Task Force (CTF) components execute missions to degrade Nevatah's ability to fight
- Lewizziland Carrier Task Force (LS Sidehorn) reinforces Blu-Blu Surface Action Group (SAG); moves north, crossing 21 degree latitude; maritime patrols increase; Defensive Counter Air (DCA) increased for port of San Diego
- CTF warns Lewizziland, demands they retire south of 21 degree latitude
- Coalition Force Maritime Component Commander (CFMCC) and Coalition Force Land Component Commander (CFLCC) provide Theater Ballistic Missile Defense (TBMD)
- Coalition Force Air Component Commander (CFACC) supports with Close Air Support (CAS), Battlefield Information (BI) and Theater Ballistic Missile (TBM) strikes; ensures local Air Superiority (AS) over Reno, Nellis operations
- CFMCC and Marine Forces (MARFOR) prepare for opposed amphibious landing, Corpus Christi
- 31st Marine Expeditionary Unit (MEU) conducts split-MEU operations; one-half element conducts Ship to Objective Maneuver (STOM) into Reno/Tahoe Airport; one-half element secures Hwy. 10 and establish defensive positions east of Kingman
- United Kingdom (UK) A Company on patrol; uncover arms cache resulting in firefight and request for CAS from UK Air Combat Command

COALITION TASK FORCE SCENARIO

U.S. European Command (USEUCOM) was the host Combatant Command for CWID 2008. The conflict notionally occured on a land mass and littoral of USEUCOM's area of responsibility (actually Western Continental United States for planning and mapping purposes). A U.S.-led CTF and a NATO joint force, NATO Response Force (NRF), comprised friendly forces. The friendly island nation of Kahuda (actually Hawaii) agreed to provide basing for interim staging and logistical requirements. The CWID 2008 scenario's theme began with a pre-existent, moderate-sized International Security Assistance Force (ISAF) conducting stabilization operations in one nation. Regional unrest then escalated to a regional multinational insurgency, cross-border

MAJOR EVENTS WHEN THE SCENARIO STARTS

- United Kingdom led International Security Assistance Force (ISAF) in place, Terrizona
- CTF Bison is in theater, Oahu, Kahuda Islands; forces marshaled; limited deployment into Area of Operations (southern Califon,Terrizona)
- NRF emplaced in area of operations (Wassegon)

DISTRIBUTED TASK FORCE ELEMENTS

COALITION TASK FORCE

U.S. EUROPEAN COMMAND (USEUCOM): Combatant Command; Coalition Task Force Commander; role plays out of Kelley Barracks, Stuttgart, Germany.

COALITION LAND COMPONENT COMMANDER (CFLCC): role plays out of Naval Surface Warfare Center (NSWC), Dahlgren, VA; U.S. Army and U.S. Marine Corps elements of the CFLCC role play out of NSWC, Dahlgren, VA.

COALITION FORCE MARITIME COMPONENT COMMANDER (CFMCC): role plays out of Space and Naval Warfare Systems Command (SPAWAR), San Diego, CA.

COALITION FORCE AIR COMPONENT COMMANDER (CFACC): role plays out of Electronic Systems Center (ESC), Hanscom Air Force Base, MA.

NATO RESPONSE FORCE

Command elements of NRF role play out of Camp Jorstadmoen, Lillehammer, Norway

NATIONAL ELEMENTS

Canada, New Zealand, and the United Kingdom role play units from their respective countries; Canada role plays homeland defense with NORAD-US-NORTHCOM, Colorado Springs, CO.

invasion and mid-intensity conflict. Destabilization, humanitarian crisis, and hostilities required the deployment of coalition task forces to re-instate regional stability.

HOMELAND SECURITY/HOMELAND DEFENSE SCENARIO

The HS/HD scenario exploited an ongoing interest in technologies that support preparation and prevention for and response to terrorist attacks and natural disasters with a focus on information sharing among federal and state military forces and federal, state and local governments. The HS/HD scenario consisted of several vignettes within NORAD and USNORTHCOM's Area of Responsibility (AOR).

Scenario vignettes provided a broad spectrum of natural and terrorist-related events. Vignettes were focused on areas of the AOR of interest to CWID participants. For instance, events in the northwest supported Canadian planning for the 2010 Olympics while events in West Virginia supported an annual state-wide exercise.

HS/HD PARTICIPATION

Scenario operations included: USNORTHCOM; U.S. Coast Guard; National Guard Bureau; National Guards of California, Colorado, Delaware, Massachusetts, New York, and West Virginia; State of West Virginia Emergency Operations Center (EOC) and EOCs of six counties; Virginia EOC; SPAWAR, San Diego; San Diego State University Visualization Lab; and the San Diego Police Department, city and county EOCs; Canada Command; and the Canadian Government Operations Centre



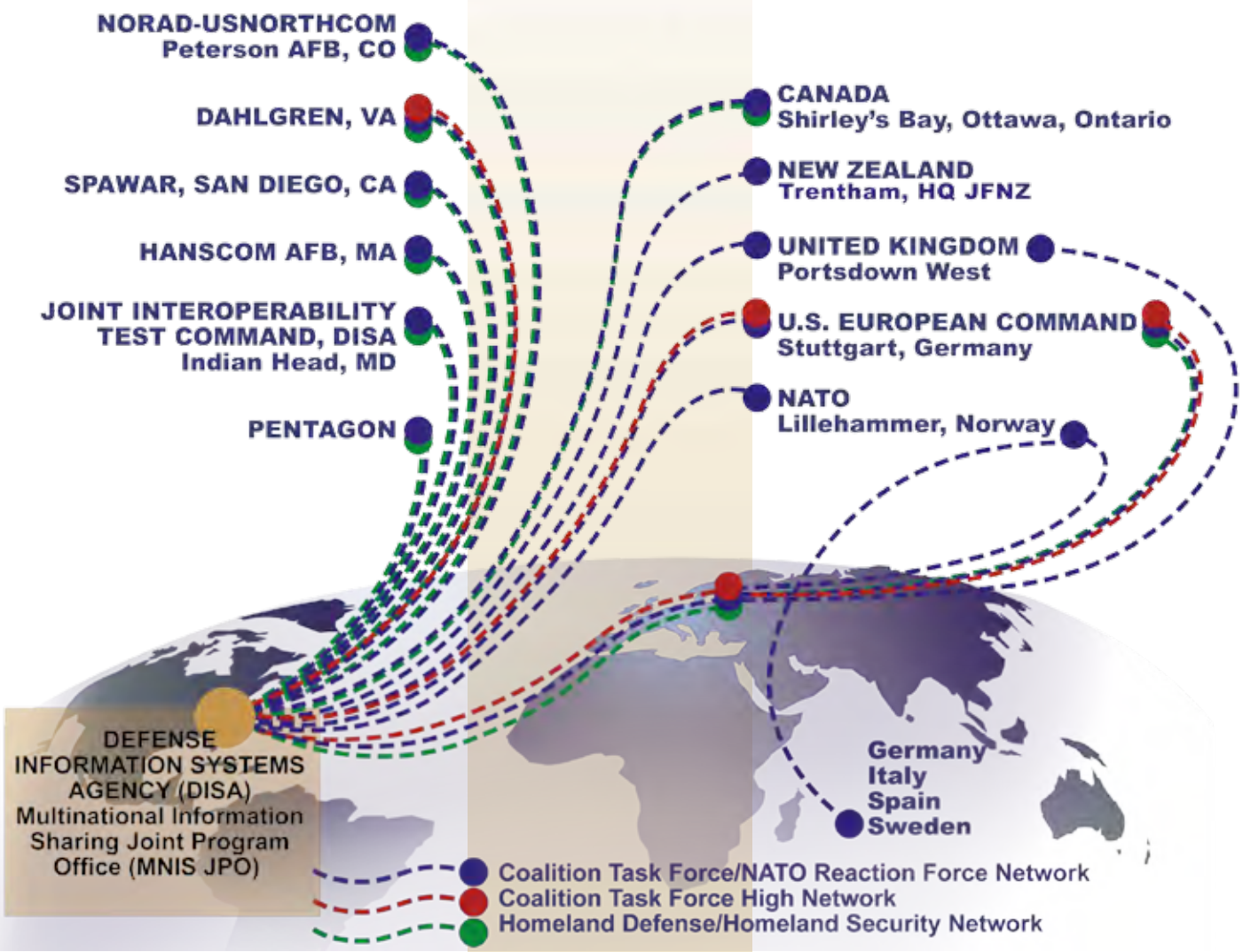
NETWORK ENGINEERING SUMMARY

A Dynamic, Global Network

The CWID network was a dynamic environment. Engineers created three security enclaves: the HS/HD, unclassified; Coalition Task Force/NATO Response Force (CTF/NRF), secret; and the CTF High, secret enclave, a notionally higher classification than CTF/NRF.

The CTF High enclave supported cross-domain-solution trials that did not use a tested guard. As a result, data could not be passed from CTF/NRF to HS/HD. Network engineers used the CFBLNet as the backbone, utilizing type-1 encryption to separate enclaves. They designed the network to be scalable, flexible and closely emulate current operational networks to demonstrate and assess new technologies, while still providing a low threat environment.

The core of the CWID network resided at the Multinational Information Sharing-Joint Program Office (MNIS-JPO) facility in Arlington, VA. Network engineers manned a Coalition Communications Control Center (known as "Quad C") at MNIS-JPO from



where they monitored network health and performance and assisted network users.

NOTABLE ACHIEVEMENTS

■ Successfully implemented an IPv6 tunnel between Dahlgren and San Diego in support of an IT, deploying Juniper WAN accelerators at all U.S. and Coalition sites on the CTF/NRF enclave multiplying network capacity up to 4 times

■ Successfully tested and deployed a new collaboration service, Adobe Connect

■ As part of the HS/HD demonstration, successfully implemented Virtual Private Networks (VPNs) to interconnect the Virginia Department of Emergency Management, West Virginia National Guard and San Diego State University

THE CTF/NRF ENCLAVE

The CTF/NRF Enclave used the CFBLNet backbone Asynchronous Transfer Mode (ATM) transport layer. Designed as a secret-releasable network for all participants, the network was capable of supporting high-speed data transmission of up to 45Mbps. In the U.S., the CTF/NRF enclave shared up to 40 Mbps bandwidth with other enclaves. The CTF/ NRF enclave connected eight U.S. and five Coalition sites. Network core services such as Domain Name Service (DNS), network timing, anti-virus signature updates and the collaboration portal, were provided by multiple countries, creating an actual coalition network environment.

CWID networks are designed to be scalable, flexible and to closely emulate operational networks.

■

THE HS/HD ENCLAVE

The HS/HD enclave shared CFBLNet transport with the CTF/NRF enclave, but only supported unclassified data. This enclave, established to support NORAD-USNORTHCOM's participation, connected all sites in the continental U.S. and one in Germany. Engineers provided Internet connectivity via dual T-1 connections (3 Mbps) over public telephone services. They also provided public e-mail, using Symantec's Single Mail Transfer Protocol (SMTP) Gateway as a filter. Extensive use of 256-bit Advanced Encryption Standard encrypted VPN tunnels allowed public first-responder participation, to include police, firefighters and National Guard operations centers. Canada and New Zealand also accessed the CWID HS/HD infrastructure.



TRIALS CONTENTS PAGE

Interoperability Trials

Coalition Warrior Interoperability Demonstration trials for 2008 are listed in trial number order below, cross referenced to sites where they were observed during the demonstration June 9 to 20.

OBJECTIVES KEY

1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ■
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ■
3. ENHANCE CROSS-DOMAIN AND MULTIPLE SECURITY LEVEL INFORMATION EXCHANGE TOOLS ■
4. ENHANCE INTEGRATED LOGISTICS PLANNING TOOLS ■
5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ■

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	USEUCOM	USNORTHCOM	DAHLGREN	SPAWAR	HANSCOM	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
1.02	Commercial Joint Mapping Toolkit Geospatial Appliance (CGA)	■		■		■		■	■		NGA	Northrop Grumman	**1**	25
1.04	Identity Based Access Device and DEFense Identity Management NETwork (IBAD/ DEFIMNET)	■	■	■	■	■	■				USNORTHCOM	Route1, Inc.	**1**	25
1.07	Joint Strike Fighter Off-board Mission Support Environment (JSF OMSE)			■		■					JSF Program Office	Lockheed Martin	**1**,2	26
1.15	IPv4-IPv6 Transformer (Datatek)			■	■						US Army	Datatek Applications, Inc	**1**	26
1.22	Army Future Combat Systems Joint Interagency Multinational Interoperability (FCS JIMI)			■					■		US Army	US Army	**1**	27
1.40	Joint Automated Deep Operations Coordination System (JADOCS)	■		■		■	■		■	■	USSOCOM	Raytheon	**1**	27
1.49	LINSE - Data Link/SA Integration via open, federated Enterprise Service Bus (LINSE)			■	■	■					German Navy	IBM	**1**,5	28
1.53	High Power X-Band Satellite Communications (XTAR)	■		■		■					DISA	Xtar LLC; L3 NARDA; DRS; SKYPORT; iDIRECT	**1**	28
1.61	ICoalition (Army Space Support Team – Tactical Set [ARRST-TS]) Prototype (CAP)	■		■		■				■	US Army	US Army	**1**,5	29
1.62	RIOS Incident Site Communications Capability (RISCC)		■	■	■						USNORTHCOM	SyTech Corp	**1**	29
1.63	Global Command and Control System/ Internet Common Operational Picture (GCCS-J 4.1.1/ICOP)	■		■	■	■	■	■	■	■	DISA	Northrop Grumman	**1**	30
1.68	Coalition open Joint Operations Picture (CoJOP)	■		■	■	■	■	■	■	■	United Kingdom	Fujitsu Services	**1**,5	30
1.72	GLOBETrekker X Band System			■		■					US Air Force	Norsat International, Inc.	**1**	31
1.79	PDA 184			■	■	■					DISA	DISA	**1**	31
2.01	Classification-Stateless, Trusted Environment (CSTE)		■	■							USSOCOM	USSOCOM	**2**	32
2.03	WorkFlow Manager and Brief Assembly Tool (WOMBAT)	■	■	■	■	■	■				US Navy	US Navy	**2**,1,5	32
2.10	Agile Client (AC)	■	■	■	■	■					DISA	Northrop Grumman	**2**	33
2.12	Collaborative Advanced Planning Environment (CAPE)			■	■	■					SPAWAR	Gnostech, Inc.	**2**	33
2.16	Joint Environment Toolkit (JET)		■	■		■	■		■		US Air Force	Raytheon	**2**	34

Continued next page



OBJECTIVES KEY

1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ■
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ■
3. ENHANCE CROSS-DOMAIN AND MULTIPLE SECURITY LEVEL INFORMATION EXCHANGE TOOLS ■
4. ENHANCE INTEGRATED LOGISTICS PLANNING TOOLS ■
5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ■

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	USEUCOM	USNORTHCOM	DAHLGREN	SPAWAR	HANSCOM	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
2.17	Search and Rescue Optimal Planning System (SAROPS)		■	■							US Coast Guard	Northrop Grumman, ASA	**2**	**34**
2.24	Hybrid Multilevel Environment (HME)			■							DISA	General Dynamics	**2**	**35**
2.26	Stealth Solutions for Networks		■								DISA	Unisys	**2**	**35**
2.27	Compartmented High Assurance Information Network (CHAIN)	■									DISA	Raytheon	**2**	**36**
2.28	Secure Information Sharing Architecture (SISA)					■					DISA	TKC Communications	**2**	**36**
2.29	Federated Identity Management System (FIdM)				■						DISA	BearingPoint	**2**	**37**
2.46	Information Integration Dashboard for Mission Support Planning (IID)				■	■	■			■	Canada	Canada	**2**	**37**
2.80	ThinSessions (TS)	■		■	■		■			■	US Joint Staff.	Northrop Grumman	**2**	**38**
2.82	Proximity-Sensitive Session-Support Services (PS4)					■					DISA	NETCONN Solutions	**2**	**38**
2.83	Agile Coalition Environment (ACE)				■						DISA	Referentia Systems Inc.	**2**	**39**
2.84	Smart Data Flow (SDF)				■						DISA	Referentia Systems Inc.	**2**	**39**
3.70	Coalition Dual Phenomenology Data Fusion-U.S. (CDPDF-US)	■									US Air Force	Missile Defense Agency	**3**	**40**
5.06	Common Information Centric Security (SecureD)	■	■	■	■		■				OSD	SPAWAR	**5**	**40**
5.14	Battlespace Terrain Reasoning and Awareness - Battle Command Commercial Joint Mapping Toolkit (BTRA-BC CJTMK) Extensions (BCE)	■		■	■						US Army	Northrop Grumman	**5**	**41**
5.18	enhanced Mobile Incident Command Post (eMICP)			■							US Coast Guard	VSE-Featherlite	**5**	**41**
5.34	Poliwall with HIPPIE Appliance (HIPPIE)		■	■	■	■					**DISA**	TechGuard Security LLC	**5**	**42**
5.48	Federated Intelligence Network (FedIntel Network)		■	■	■	■	■				USNORTHCOM	CompuSat Services, Inc.	**5**	**42**
5.59	Coalition Dual Phenomenology Data Fusion - USNORTHCOM (CDPDF-USNORTHCOM)										USNORTHCOM	Missile Defense Agency	**5**	**43**
5.64	Trusted Enterprise Services Bus (T ESB)	■	■	■	■	■	■	■			DISA	World-Wide Consortium for the Grid (W2COG) Institute	**5**	**43**
5.65	Security Information Management for Enclave Networks (SIMEN)		■	■		■					US Air Force	The MITRE Corp.	**5**	**44**
5.73	VirtualAgility OPS Center (VOC)		■	■	■		■				Canada	IBM, VirtualAgility Inc.	**5**	**44**
5.81	Transnational Information Sharing Coalition (TISC)	■	■	■						■	US Army, US Navy, DISA	US Army, US Navy, DISA	**5**	**45**
	History of Coalition Warrior Interoperability Demonstration													**46**
	CWID Heritage of Delivering Capabilities to the Warfighter													**47**

IT 1.02

Commercial Joint Mapping Toolkit Geospatial Appliance

1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: CGA, a hardware and software configuration, provided administrative capabilities for Limited Distribution NGA geospatial data in an application-ready data format for the defense and intelligence communities. Geonames, Natural View data and Environmental Systems Research Institute (ESRI) globes were available with additional products. CGA provided net-centric access using open protocols and standards, Simple Object Access Protocol (SOAP) for ESRI products, and the OGC WMS. Systems requiring direct access to geospatial data connected to CGA and accessed data in their native format or method. Dahlgren used a rack-mounted configuration designed for a high volume of simultaneous users while USEUCOM used a ruggedized version designed for fielded environments.

SPONSOR:
NGA

LOCATIONS:
USEUCOM
NSWC Dahlgren
New Zealand

PARTNERS:
IT2.10
IT5.14

ASSESSMEMT RESULTS::
CGA operated on the CTF domain and received an Information Assurance (IA) assessment and a SEIWG evaluation.

CGA successfully demonstrated Objective 1.

- Offered Web Mapping Services with Open Geospatial Consortium specifications and ESRI OpenGIS software with deliverable hardware devices.
- Integrated geospatial services to multiple CWID systems and technologies.
- Maintained an adequate IA security posture. Some vulnerabilities and open ports/services were noted for correction in future releases.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.04

DEFense Identity Management NETwork and Identity Based Access Device - Common Access Card

1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: MobiKEY IBAD provides portable, high assurance remote access to C4ISR systems and information from anywhere. Secure communication capabilities were powered by DEFIMNET, a fault-tolerant, highly scalable identity/entitlement management infrastructure designed to deter infiltration and penetration of adversarial reconnaissance, surveillance, and information operations. IBAD's compact form-factor provides portability, eliminating the need for field personnel to carry laptops that could potentially land in enemy hands. IBAD-C, designed to accept DoD-sanctioned Common Access Cards (CAC), extended authentication to include Windows. Employing existing battlefield or naval networks for connectivity, MobiKEY IBAD or IBAD-C provided secure reachback to command and control decision makers.

SPONSOR:
USNORTHCOM

LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
Canada

PARTNERS:
None

ASSESSMEMT RESULTS:
DEFIMNET IBAD/ IBAD-C operated on the HS/HD and CTF domains and received a Warfighter, Technical/Interoperability, and an Information Assurance (IA) assessment.

DEFIMNET IBAD/ IBAD-C successfully demonstrated Objective 1.

- Provided deployed users an effective secure communications device for full access to important documents and crucial data from a host computer.
- Operators successfully logged onto a host machine from a remote machine using the CAC credentials and worked as if they were located at the host machine. Operators used email and other standard desktop applications, logged into Adobe Connect sessions, and used functions like chat and document retrieval and sharing.
- Remotely launched C2PC and generated reports successfully.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.07

Joint Strike Fighter Off-board Mission Support Environment

1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ● 2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: JSF's OMSE is a ground-based mission planning system designed to support all aspects of coalition mission preparation and post mission analysis. The trial provided Horizontal and Vertical Collaborative Mission Planning, Electronic Warfare analysis, and Mission De-confliction for resolving chronological and geospatial (4D) conflicts between multiple aircraft operating within a fixed airspace. It also provided an improved hardware/software suite for Cross Security Domain Data Exchange.

SPONSOR:
Joint Strike Fighter Program Office

LOCATIONS:
NSWC Dahlgren
ESC Hanscom

PARTNERS:
IT2.12
IT1.68
IT2.16

ASSESSMEMT RESULTS:
JSF OMSE operated on the CTF domain and received a Warfighter, Technical/ Interoperability and Information Assurance (IA) assessment.

JSF OMSE successfully demonstrated Objective 1 and 2.

- Demonstrated data compatibility with various mission data formats: Air Tasking Order and Airspace Control Order in .txt and .aco/.ato formats, Order of Battle in .thr and Joint Mission Planning System Framework Backup formats, and strike coordination data in .f35, .jrt, and .crd formats.
- Demonstrated collaborative planning and dissemination of mission planning products in a bandwidth constrained environment.
- Used the Autonomic Logistics Information System server to securely interface with the Collaborative Advanced Planning Environment (CAPE) server and Dashboard Man Machine Interface.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.15

IPv4-IPv6 Transformer

1. IIMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: The IPv4-IPv6 Transformer instantly converts IPv4-only legacy systems into dual-stack IPv4/IPv6 systems, to enable IPv6 messaging, while preserving IPv4 pass-through mode. The IPv4-IPv6 Transformer adds Mobile IPv6 and Information Assurance functions such as IPsec and IKE to legacy IPv4-only systems. A transparent solution with no software or hardware changes, the trial extends the continued operation of IPv4 legacy equipment and applications until expected replacement. The IPv4-IPv6 Transformer enables seamless network transition from IPv4 to IPv6 at the time of the customer's choosing, no network 'flash cuts' required. A dual-stack IPv4/IPv6 network enables transmission of IPv6 messages between IPv4-only fire support systems through AFATDS, NFCS and JADOCS.

SPONSOR:
US Army

LOCATIONS:
NSWC Dahlgren
SPAWAR

PARTNERS:
None

ASSESSMEMT RESULTS:
IPv4-IPv6 Transformer operated on the CTF domain and received an Information Assurance (IA) assessment and a SEIWG evaluation.

IPv4-IPv6 Transformer successfully demonstrated Objective 1.

- Integrated within a dual IPv4-IPv6 network architecture utilizing an easy-to-use menu system.
- Accelerated network migrations to IPv6 by providing a seamless and transparent solution for legacy IPv4 systems and applications.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.22

Army Future Combat Systems Joint Interagency Multinational Interoperability

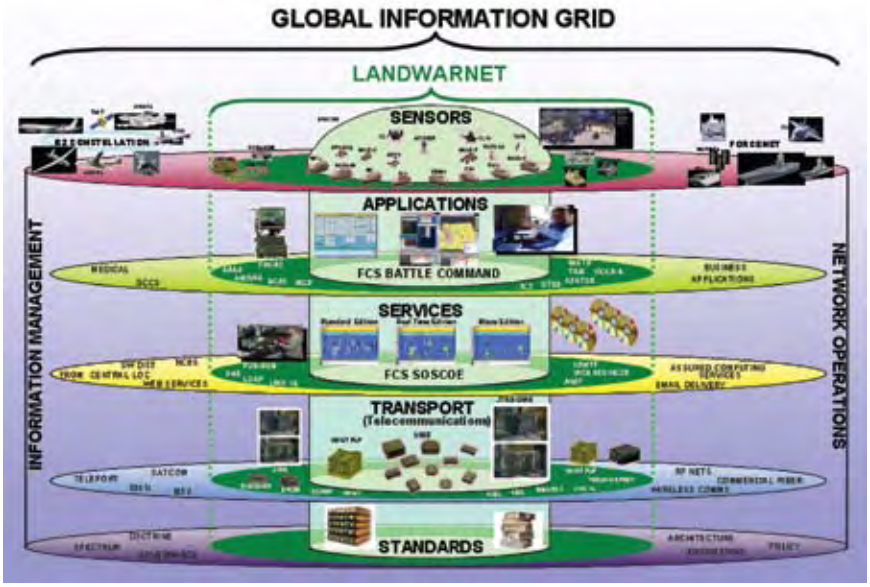
1. IIMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: The FCS Brigade Combat Team (BCT) Program is the Army's primary modernization effort. FCS, a family of manned ground vehicles, unmanned aerial and ground platforms, and sensors are connected by a common network. Through the FCS Network, warfighters' situational awareness, protection, and lethality is improved. FCS provides interoperability capabilities of its maturing services, standards and applications to conduct Situational Awareness (SA) data exchange, collaborative operations, and targeting missions with a particular focus on information exchange with UK Systems. The FCS System of Systems Common Operating Environment (SoSCOE) and FCS Battle Command are the critical Army components that enable network-centric operations and interoperability to numerous US Joint and Coalition Systems.

SPONSOR:
US Army

LOCATIONS:
NSWC Dahlgren
United Kindom

PARTNERS:
None



ASSESSMEMT RESULTS:
FCS JIMI operated on the CTF domain and received an Information Assurance (IA) assessment and a SEIWG evaluation.

FCS JIMI met Objective 1.

- Performed risk mitigation testing the System of Systems Common Operating Environment (SoSCOE) interoperability between the US and UK.
- Defined finite requirements by exploiting US to UK connectivity with LC2IS.
- Interfaced with standard DoD services.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.40

Joint Automated Deep Operations Coordination System

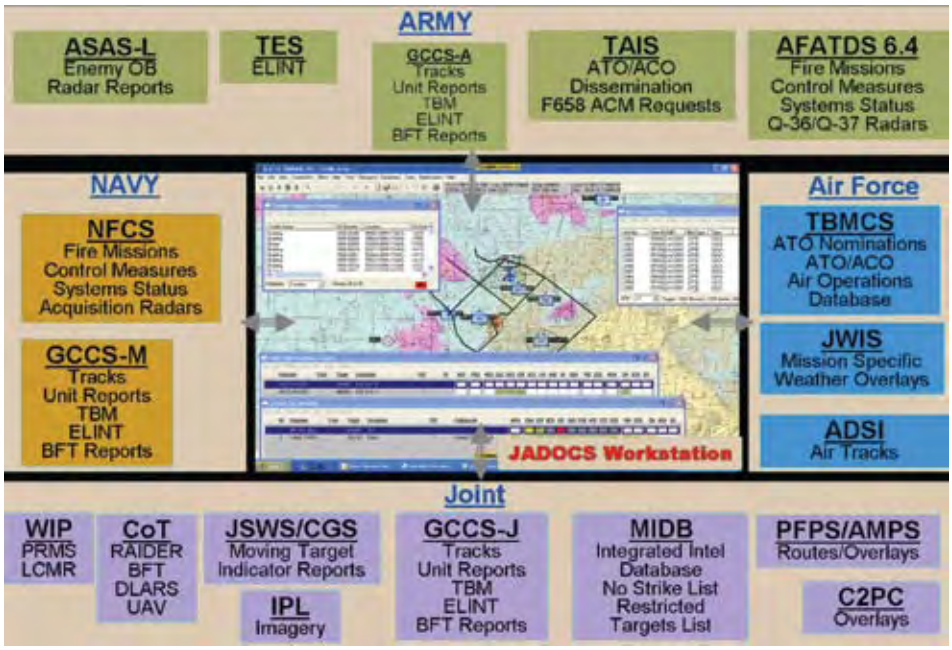
1. IIMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: JADOCS provides a suite of system interfaces to multiple sets of Command and Control (C2) data that allows the user to access and manipulate data as required to accomplish C2-related tasks. JADOCS also provides a set of unique mission management consoles that allow key decision makers to streamline the coordination and mission approval process.

SPONSOR:
USEUCOM

LOCATIONS:
USEUCOM
NSWC Dahlgren
ESC Hanscom
Canada
NATO

PARTNERS:
IT 1.61



ASSESSMEMT RESULTS:
JADOCS operated on the CTF domain and received a Warfighter and Technical Interoperability assessment.

JADOCS was marginally successful meeting Objective 1. Real world events prevented JADOCS from providing adequate support to demonstrate CWID Objectives.

- Coalition review of the latest revision of JADOCS software across Canada, United Kingdom, NATO, and Unites States operators.
- Successfully received and displayed a GPS prediction report shape file from IT 1.61.
- JADOCS role-players were unable to provide sufficient data to accurately assess the trial.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.49

Data Link/Situational Awareness integration via open, federated Enterprise Service Bus

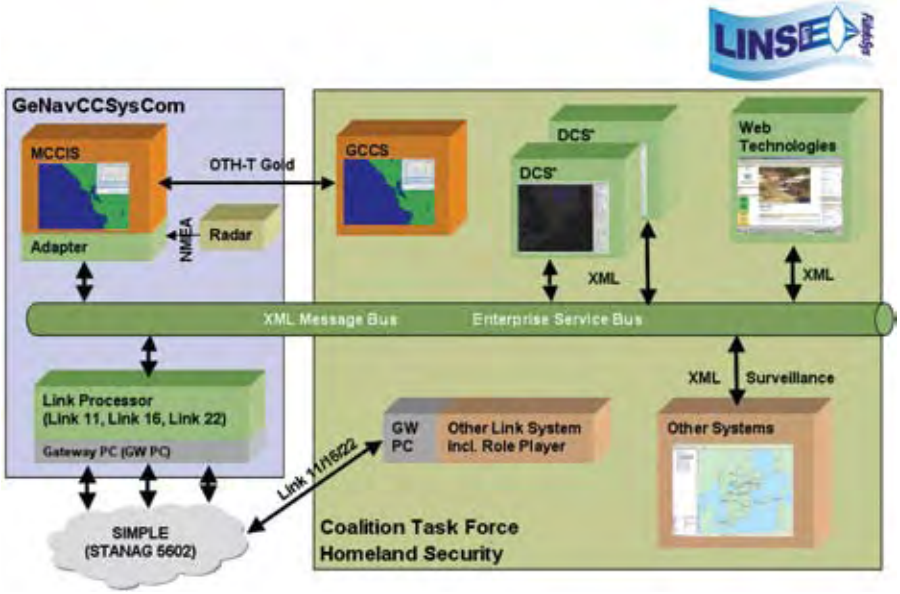
1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ● 5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: LINSE uses commercial off-the-shelf (COTS) messaging technology to facilitate interoperability between platforms that have tactical data link (TDL, L11/M-Series, L16/J-Series, L22/F- and FJ-Series) legacy systems, OTH-Gold systems and platforms or sites that are TCP/IP-enabled. LINSE integrates TDL information with data from other sources (e.g., intelligence or logistics systems) and improves mission performance through a richer operational picture available to all mission participants. LINSE enhances leadership's capability to command, control and coordinate across joint and coalition forces, government agencies, non-government organizations (NGOs) and first responders.

SPONSOR:
German Navy

LOCATIONS:
NSWC Dahlgren
SPAWAR
ESC Hanscom

PARTNERS:
None



ASSESSMEMT RESULTS:
LINSE operated on the CTF domain and received a Warfighter, Technical /Interoperability, and Information Assurance (IA) assessment.

LINSE successfully demonstrated Objective 1 and 5.

- Received and converted track data types: Link 16 (J-Series), Link 22, OTH Gold, XML, NMEA radar tracks for display on other systems with connection to LINSE - Global Command and Control System (GCCS), Internet Common Operational Picture (ICOP), Display and Control System (DCS), and Air Defense Systems Integrator (ADSI).
- Exchanged Link 16 command and free text messages with ADSI.
- Used Service Oriented Architecture (SOA) to open new data feeds to the COP and provided Tactical Data Link capabilities to applications which previously had none.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.53

High Power X-Band Satellite Communications

1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: XTAR offers two major features: very high data rates of 155mb/s links and "Comms-on-the-Move" from small lightweight, low-cost mobile terminals. Applications also include video teleconference (VTC). XTAR demonstrates the benefits of high power X-band using the Army National Guard's new X-band SATCOM as a basis of a National Emergency SATCOM Network – interface with USCG first responder command post. Key technologies include DRS (18" XOTM terminal), L3 NARDA (1.6m and 3.9m terminals), iDIRECT (IP-based network), Army JOIN VTC and Multi-band Teleport.

SPONSOR:
DISA

LOCATIONS:
USEUCOM
NSWC Dahlgren
ESC Hanscom

PARTNERS:
IT 5.18

ASSESSMEMT RESULTS:
XTAR operated on the HS/HD domain and received a Technical/Interoperability assessment.

XTAR successfully demonstrated Objective 1.

- Demonstrated data access, fusion & integration among joint forces, international, Federal and State Agencies & local law enforcement and demonstrated open and secure mobile C2 capabilities between communities of interest (COIs).
- Set-up and operated Video Teleconferencing (VTC) capabilities through Skyport located in Houston with little latency and no issues.
- Demonstrated VTC's, streaming video, and the Ku- to X-band Cross Band Solution within the Coast Guard Emergency Mobile Incident Command Post.
- Used the ViaSat demonstration at Dahlgren to successfully demonstrate streaming video and cross-band connectivity.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.61

Coalition (Army Space Support Team - Tactics Set [ARRST-TS]) Prototype

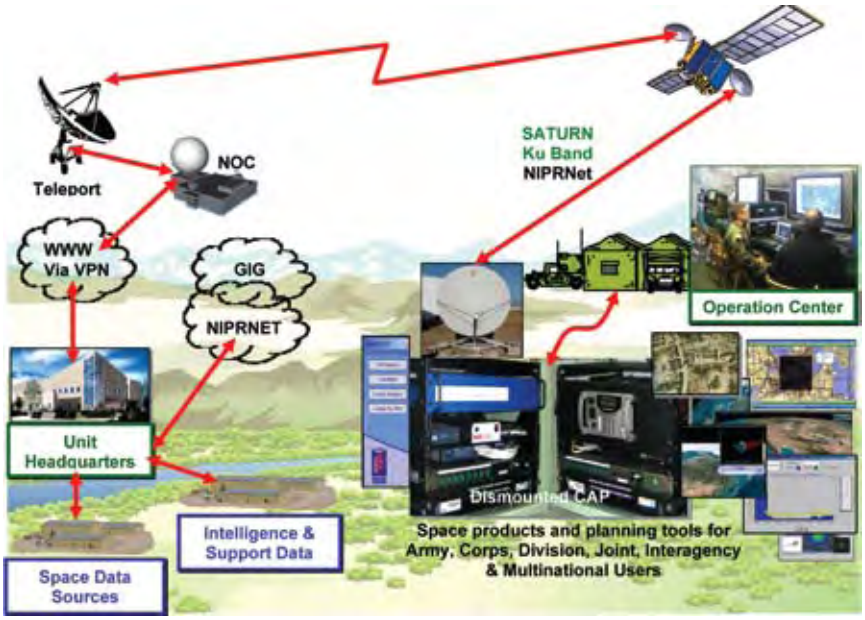
1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ● 5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: CAP provides the ability to garner, analyze and disseminate relevant space data and information. CAP enables operationally relevant space planning tools and mission execution support data for the joint, interagency or multinational user. CAP consists of two major subsystems: the Space Applications Technology Utility Research Network (SATURN) and the Space Operations Systems (SOS). The SATURN provides global reachback through triple redundant global commercial satellite data and voice internet protocol (IP) satellite, International Marine/Maritime Satellite (INMARSAT) and Iridium. Voice through IP provides commercial switching capability. The SOS is a commercial laptop workstation with a customized suite of commercial and government software applications and capabilities.

SSPONSOR:
US Army

LOCATIONS:
USEUCOM
NSWC Dahlgren
ESC Hanscome
NATO

PARTNERS:
IT 1.40



ASSESSMEMT RESULTS:
CAP operated on the CTF domain and received a Warfighter and Technical /Interoperability assessment.

CAP successfully demonstrated Objectives 1 and 5.

- Prototype system currently used by CENTCOM that allowed military leaders to command more efficiently by using commercial satellite imagery instead of reconnaissance units
- Provided senior leadership with GPS satellite over flights information, helping mission planning and collaboration between joint and coalition forces, government agencies, NGOs and first responders
- Demonstrated a situational awareness tool that used advanced visualization technologies capable of integrating existing systems into JADOCS COP, streamlining decision-making
- Operators gathered space and or terrestrial weather information on operational activities and forwarded the data via Power Point presentation to senior leadership.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.62

RIOS Incident Site Communications Capability

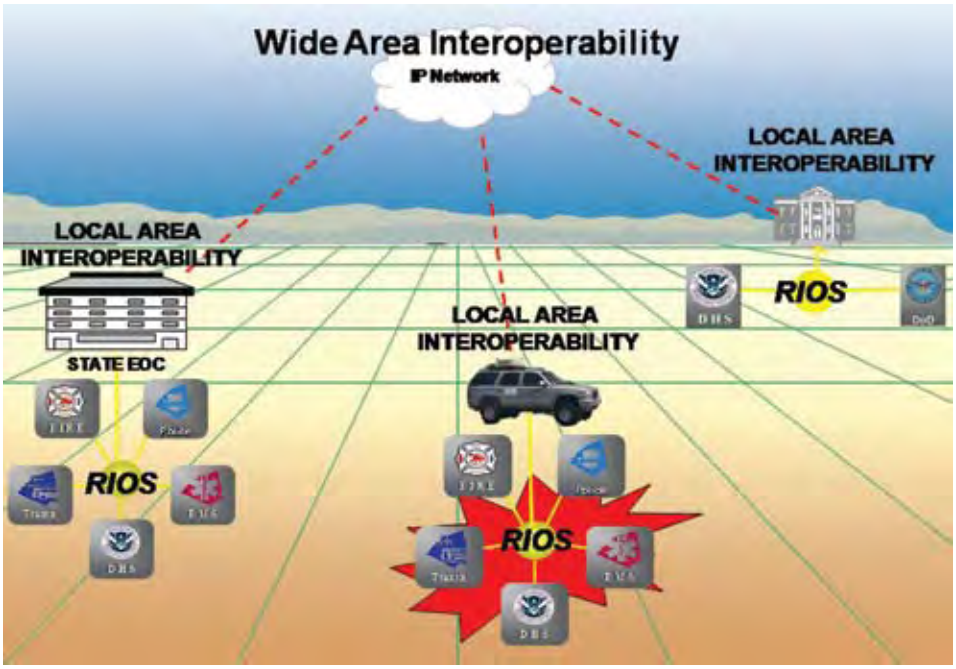
1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: RISCC provides both local and wide area interoperability with enhanced command and control features; remote radio control, logged RIOS chat, remote site operations, incident recording, playback and reporting. The system operates with civilian and military communications devices including radios, phones, and computers and legacy devices and connects civilian agencies, first responders and military units. RISCC features an easy to use and easy to train Graphical User Interface (GUI) that enhances situational awareness.

SPONSOR:
USNORTHCOM

LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR

PARTNERS:
None



ASSESSMEMT RESULTS:
RISCC operated on the HS/HD domain and received a Warfighter, Technical/ Interoperability and Information Assurance (IA) assessment.

RISCC successfully met Objective 1.

- Created cohesive talk group linkages over UHF and VHF radio, cellular phones, and VoIP between military and government agencies. Transmitted voice and text via one Internet Protocol address.
- Demonstrated communications tools via an easy to use touch screen panel over a wide area network, aiding situational awareness and decision making.
- RISCC increased communication interoperability across the country, efficiently and effectively supporting different users including Defense Support of Civil Authorities. Connected the San Diego State University RIOS terminal to a local Fire Department and monitored live DC and VA incidents.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT

BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.63

Global Command and Control System/Internet Common Operational Picture

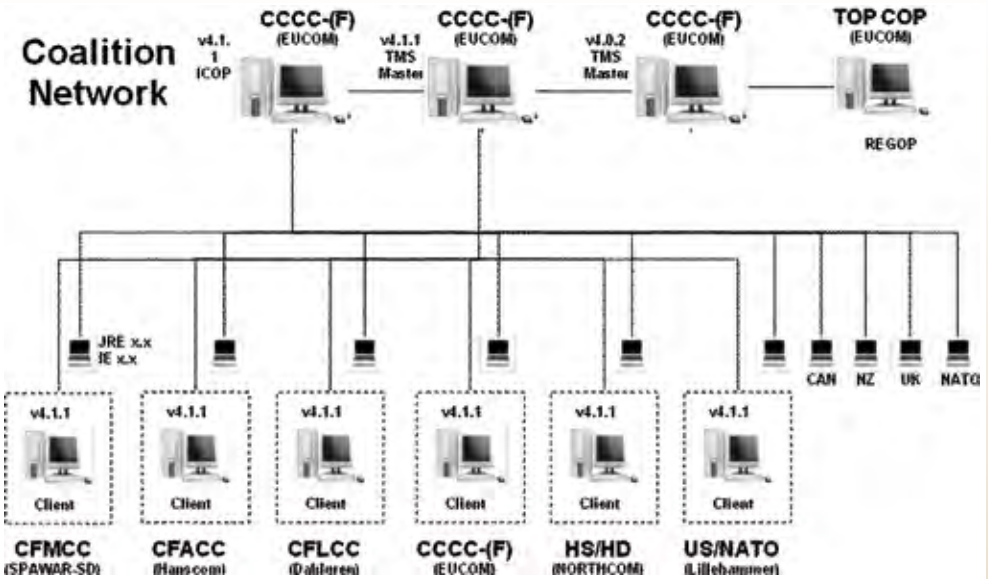
1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: GCCS-J 4.1.1 ICOP platform is a significant migratory step toward a service-oriented architecture in the situational awareness and command and control arena within the joint warfighting community. This trial demonstrates successful integration of GCCS-J 4.1.1 and ICOP in support of traditional COP Infrastructure and supports data dissemination and sharing for NATO, Coalition, and US Forces. ICOP establishes a capability that allows for track dissemination to remote sites with disadvantaged clients that can only leverage web browsers and Java packages on windows host machine.

SPONSOR:
DISA

LOCATIONS:
USEUCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
Canada
New Zealand
NATO

PARTNERS:
IT 1.02
IT 1.49
IT 1.68
IT 2.10



REPORT LINKS
FULL TRIAL REPORT

BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

ASSESSMEMT RESULTS:
ICOP operated on the CTF domain and received a Warfighter and SEIWG evaluation.

GCCS-J 4.1.1 ICOP partially demonstrated Objective 1.

- Expanded integration of open standards Service Oriented Architectures enhancing situational awareness, data dissemination, and information sharing with NATO, Coalition, and US Forces.
- Demonstrated compatibility with standard workstations.
- Experienced operational limitations with JAVA Runtime Environment (JRE), Internet Explorer and Mozilla browsers packages but worked best with Mozilla.
- Integrated with one server in EUCOM, resulting in users suffering from latency and refresh issues.
- Warfighters indicated a preference for ICOP as an operational system with performance improvements.

IT 1.68

Coalition open Joint Operations Picture

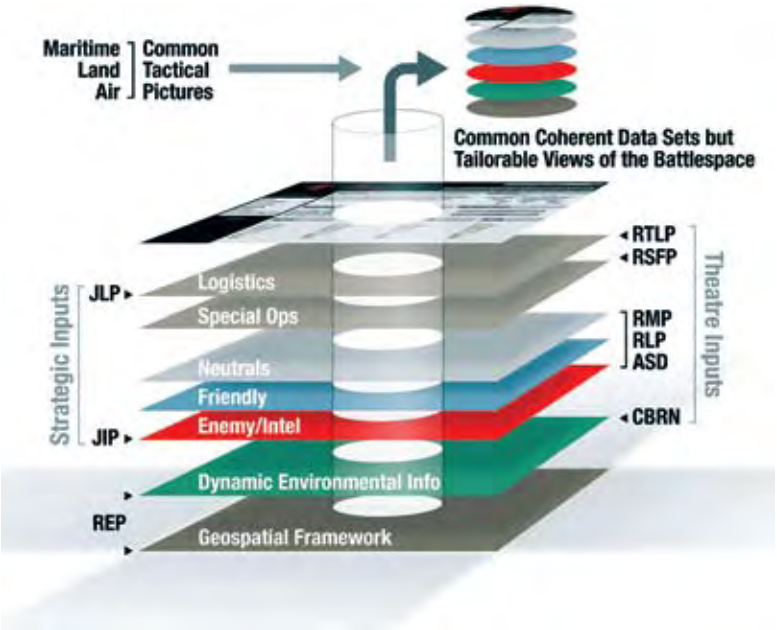
1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ● 5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: CoJOP is the coalition deployment of open JOP that delivers the Joint Operations Picture (JOP) on the UK Defence Information Infrastructure (DII) as part of the Joint Command and Control Support Programme (JC2SP). The JOP consists of the Common Operations Picture (COP) and JOPWeb, a tool that collates operational reports and returns the most current information. JOP provides shared Situational Awareness (SA). CoJOP's ability to generate, access and protect information, and its ability to share it throughout the network, allows force elements to operate from common datasets (or 'pictures') that are consistent throughout the operating space, and draw on the same underlying environmental and reference information.

SPONSOR:
Unite Kingdom

LOCATIONS:
USEUCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
Canada
New Zealand
United Kindom
NATO

PARTNERS:
None



REPORT LINKS
FULL TRIAL REPORT

BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

ASSESSMEMT RESULTS:
CoJOP operated on the CTF domain and received a Warfighter and Technical Interoperability assessment.

CoJOP was moderately successful meeting Objectives 1 and 5.

- Provided the ability to easily create, upload, and edit documents, making CoJOP a useful tool for inter agency governmental document sharing.
- Insufficient training, inadequate technical support, configuration/set-up/log-on issues, and United Kingdom firewall access issues limited the trial's overall effectiveness/success.
- Warfighters experienced access issues throughout the demonstration with CoJOP's internal links (WebS2AT, SKIP, Threat Status, JOBWEB and Link 16).

IT 1.72
GLOBETrekker X Band System

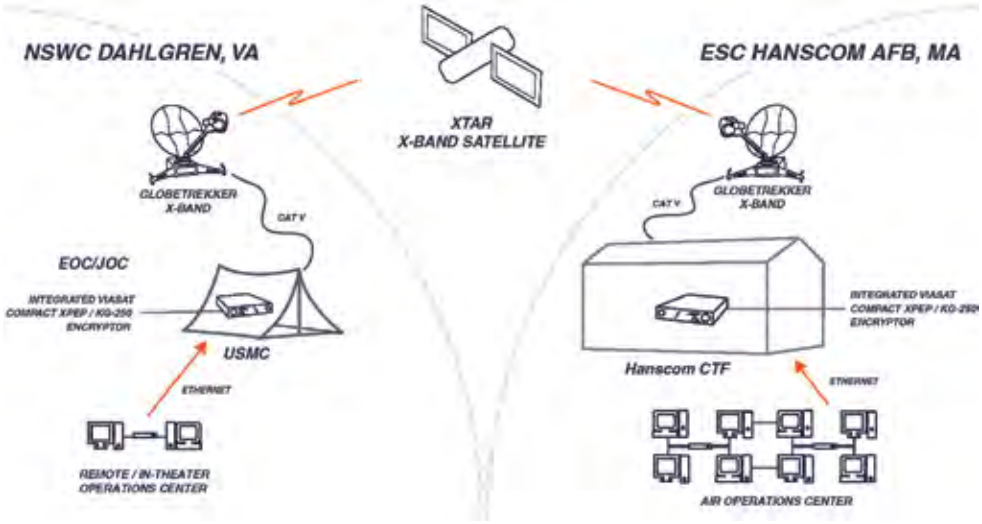
1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: GT-X-represents the next generation ultraportable, man-packable satellite system enabling broadband communications on-the-pause, offering auto-acquiring technology and LinkControl software for non-technical and technical warfighters. The terminal comes with a 1.0m antenna and is capable of operating with the U.S. WGS satellites, UK's SKYNET fleet and XTAR. When terrestrial communications are unavailable during warfighting, a secure satellite link between command and component levels enable missions to exploit a common operational picture for enhanced coordination, execution, and situational awareness. Two GLOBETrekker X-Band™ systems transport information over the XTAR satellite. Interoperating with the XTAR satellite, the compact GLOBETrekker X-Band™ system quickly transmits and receives high bandwidth information, including: maps, weather data, UAV imagery and video, and operational graphics.

SPONSOR:
US Air Force

LOCATIONS:
NSWC Dahlgren
ESC Hanscom

PARTNERS:
IT1.53



ASSESSMEMT RESULTS:
The GLOBETrekker X Band Trial operated on the CTF domain and received a Warfighter and Technical Interoperability assessment.

GT-X successfully demonstrated Objective 1.

- Provided a secure 4Mbs SATCOM link extending Hanscom's CTF Network to Dahlgren.
- Interoperated with XTAR satellite to quickly transmit and receive high bandwidth information including: maps, weather data, operational graphics, UAV imagery, and video.
- Employed Adobe Connect Collaboration capabilities, Voice over Internet Protocol (VoIP), and E-Mail with little to no latency.
- Streamlined communications with straightforward interfaces, provided reduced familiarization training, and demonstrated reliable bandwidth-intense Command and Control operations.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 1.79
Personal Digital Assistant 184

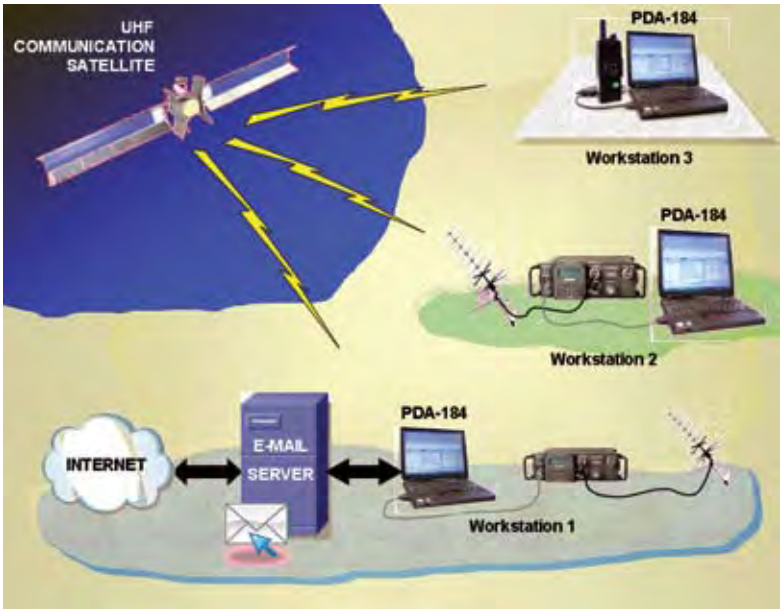
1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ●

TRIAL OVERVIEW: The PDA-184 is a man-portable software based application that allows war fighters on-the-move to communicate data using tactical UHF radios with guaranteed delivery of data, error free, at fastest possible speed for low bandwidth tactical RF communication links. The PDA-184 software runs on a laptop connected to a tactical radio (a PDA-184 workstation consists of the radio and the laptop). The PDA 184 allows the warfighter on-the-move to communicate with other warfighters using Microsoft Outlook email (Outlook modified to work in UHF SATCOM environment). In addition to email, a PDA-184 chat graphical user interface is used for direct file transfers (up to 3 MB) and text messages between PDA-184 workstations. The PDA-184 implements a UHF SATCOM standard (MILSTD-188-184) but can also be used for line-of-sight and other tactical RF communication.

SPONSOR:
DISA

LOCATIONS:
NSWC Dahlgren
ESC Hanscom

PARTNERS:
IT 2.16
IT 5.18



ASSESSMEMT RESULTS:
The PDA Trial operated on the HS/HD and CTF domains and received a Warfighter and Technical Interoperability assessment.

PDA-184 successfully demonstrated Objective 1 on the HS/HD domain.

- Passed weather data in PDF format using PDA 184 chat functionality.
- Exchanged imagery via email.
- Demonstrated ease of setup and teardown of system hardware.
- Test cases on the CTF domain were not executed due to the unavailability of the correct cryptographic key which was beyond the control of the trial.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.01
Classification Stateless, Trusted Environment

2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: CSTE is a dynamic collaborative environment for sharing information and capabilities from/to anywhere. It provides user access to information from a spectrum of network environments operating at multiple security levels and/or user groups Dependent upon user privileges, including unplanned but authorized users, CSTE allows users to control access and share information (i.e., data objects) between various classification levels and communities of interest (COI). Manages authorized users' ability to discover and access data, changing/suspending user. CSTE also demonstrates access privileges in near real time while denying data discovery/access by unauthorized users.

SPONSOR:
USSOCOM

LOCATIONS:
NSWC Dahlgren

PARTNERS:
IT 5.65

ASSESSMEMT RESULTS:
The CSTE Trial operated on the CTF and received a Warfighter, Technical Interoperability and Information (IA) Assurance assessment.

CSTE successfully met Objective 2.

- Demonstrated a role based security infrastructure.
- Provided network administrators the functionality to downgrade or upgrade warfighter's USB tokens, allowing warfighters to share information between and among coalition partners.
- Demonstrated ease in retrieving and viewing files, decrypting and encrypting files, updating, retagging, forwarding, and storing files.
- Allowed users to access, modify, and share information at classification levels from unclassified to top secret using a USB token.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.03
WorkFlow Manager and Briefing Analysis Tool

2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: WOMBAT allows globally dispersed teams to feed information into a centralized portal that manages workflow and gathers, collates, and renders information into a consistent output format. The workflow manager enables the controller to quickly and accurately determine team status. Real-time updates ensure that the controller is always aware of the current situation. Each team member's state is alphabetized and auto-sorted by importance and briefing order. WOMBAT's briefing assembly function enforces specified layouts. Unauthorized content changes are eliminated through authentication, permissions, and a centralized approval process. WOMBAT's thin client design minimizes bandwidth and does not allow installs on the client side. WOMBAT is built using a Services Oriented Architecture (SOA) and has the flexibility to be easily reconfigured.

SPONSOR:
US Navy

LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
Canada

PARTNERS:
None

ASSESSMEMT RESULTS:
The WOMBAT Trial operated on the HS/HD domain and received a Warfighter and Technical Interoperability assessment.

WOMBAT successfully demonstrated Objective 2.

- Provided an excellent tool for PowerPoint presentations with a simplified and systematic method of arrangement, allowing consolidation of briefings in a matter of minutes.
- Eliminated unauthorized and unapproved briefing changes using authentication, permissions, and a centralized approval process.
- Provided situational awareness by allowing warfighters to participate in daily briefings using the workflow manager; also allowed review and data manipulation with approval and rejection capabilities.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.10
Agile Client

1. IMPROVE COALITION AND JOINT C4ISR ARCHITECTURE ● 2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ● 5.. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: AC is a 3D COP workstation that employs open standards to access data and employ capabilities from web services using orchestration of machine-to-machine communication over a C2 services oriented architecture (SOA) and automation which reduces workload, increases accuracy, and compresses the timeline by managing mission tasks in a workflow as part of a collaborative community of interest. AC introduces patterns for subscription to data services including web services and distributed caching services. AC is constructed so that all contributing components to the end state client can be deployed over the network and composed locally.

SPONSOR:
DISA

LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
Canada

PARTNERS:
IT 1.02
IT 1.63
IT 1.68

ASSESSMEMT RESULTS:
AC operated on the CTF and HS/HD domains and received a Warfighter, Technical /Interoperability and Information Assurance (IA) assessment.

AC was moderately successful demonstrating Objectives 2, 1 and 5.

- Provided a framework for aggregation of chat, JEM, NEMXS and freeware applications during execution.
- Received plume data from Joint Effects Model (JEM) and correctly displayed on their common operational picture.
- Poor planning and lack of coordination prior to execution resulted in inefficacious performance of AC. Training was inadequate, multiple software patches were required during execution, and web-services provided by the trial were not fully functional.
- Maintained a good IA security posture. Some open ports/services noted for correction in future releases.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.12
Collaborative Advanced Planning Environment

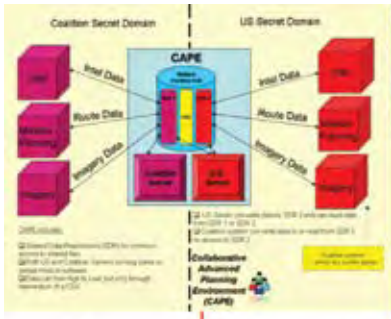
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: CAPE serves as multi-network, multi-level security data repository providing a secure portal environment to enhance collaboration between Coalition and US end-users. End-users are defined as mission planners, intelligence analysts, imagery analysts, or command and control operational analysts. CAPE's portal environment can become a critical tool in the end-users toolset toward the exchange of relevant situational awareness data.

SPONSOR:
US NAVY

LOCATIONS:
NSWC Dahlgren
SPAWAR
ESC Hanscom

PARTNERS:
IT 1.07
IT 1.68
IT 2.16



CAPE OPERATIONAL DIAGRAM

CAPE DASHBOARD

CAPE PROVIDES ENHANCED DATA SHARING AND COLLABORATION BETWEEN WARFIGHTERS LOCATED ON SEPARATE SECURITY DOMAINS

ASSESSMEMT RESULTS:
The CAPE Trial operated CTF domain and received a Warfighter, Technical/ Interoperability and Information Assurance (IA) assessment.

CAPE successfully demonstrated Objective 2.

- Collaboration consisted of voice, chat, file sharing and ease of use.
- 3-D visualization tools supporting one security domain and provided end users essential planning tools with minimum technical issues.
- Used .crd and .jrt file types within the 3D route de-confliction tool and a CAPE-centric collaboration tool and Dashboard Man Machine Interface (MMI) to demonstrate interoperability with other mission planning systems.
- Maintained an adequate IA security posture. Some minor vulnerabilities and open ports/services noted for correction in future releases.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.16
Joint Environment Toolkit

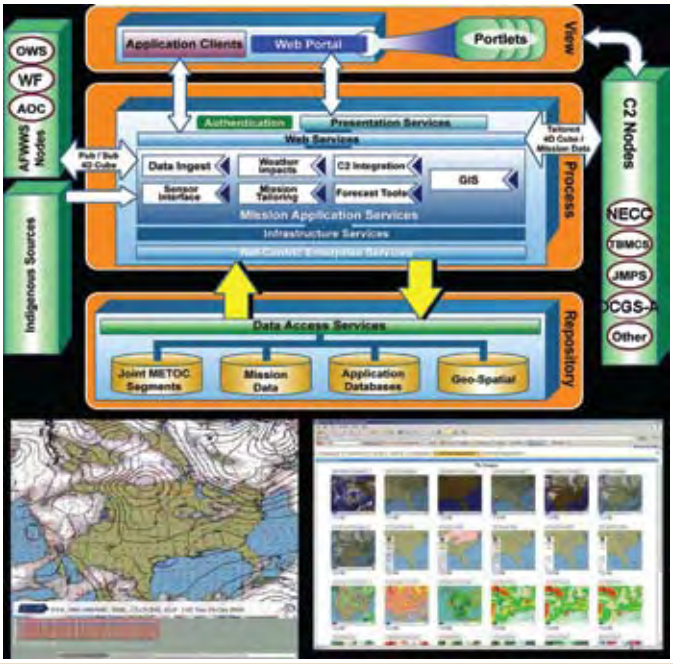
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: The Joint Environmental Toolkit (JET), a web-based weather-planning tool, provides access to common Meteorological and Oceanographic (METOC) data via portals, thick clients, and web information services. JET also allows users to get weather observations, forecasts, satellite imagery, radar, warnings, and gridded weather models. The system provides standards-based information services, Service Oriented Architectural framework, customizable Portal Interface, Really Simple Syndication (RSS) feeds, Internet Mapping Service (ArcIMS), and leverages C/JMTK technology for Geospatial Imagery Services.

SPONSOR:
US Air Force

LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
Canada
New Zealand
United Kindom

PARTNERS:
IT 1.79



ASSESSMENT RESULTS:
JET operated on the CTF and HS/HD domains and received a Warfighter, Technical /Interoperability and Information Assurance (IA) assessment.

JET successfully demonstrated Objective 2.

- Demonstrated a web-based weather-planning tool that provided current observations and forecasted weather information-at geographically separated locations.
- Warfighters requested, posted, and downloaded weather information for user-defined areas of interest on both the HS/HD and CTF networks via the JET portal.
- Provided a user-friendly interface that allowed warfighters to organize weather data via Adobe Portable Document Format (PDF) or Microsoft Office Power Point to suite their individual location needs.
- Maintained a good IA security posture. Some open ports/services noted for correction in future releases.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.17
Search and Rescue Optimal Planning System

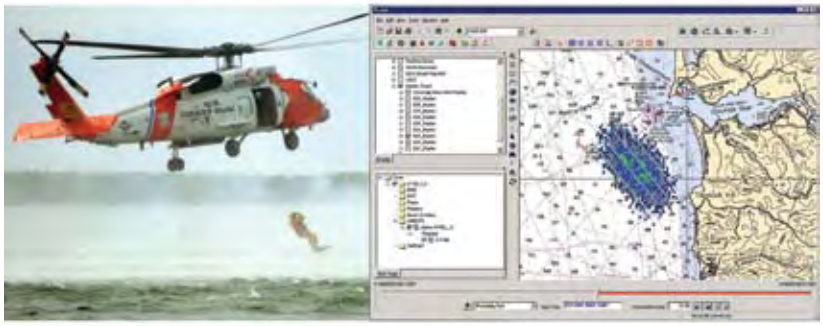
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

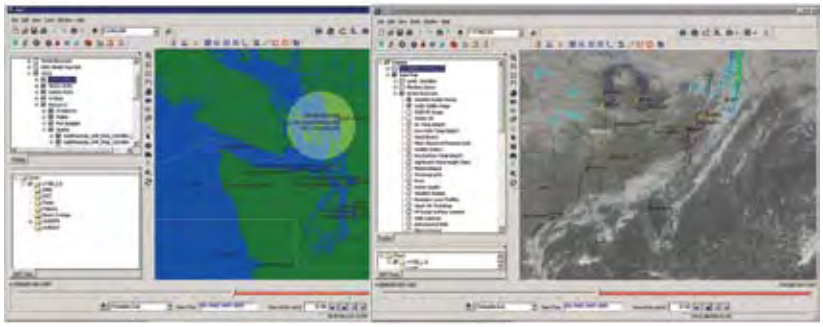
TRIAL OVERVIEW: SAROPS is the Coast Guard's primary Search and Rescue (SAR) planning tool. SAROPS is a Mission Essential Application (MEA) that operates within the standard workstation environment to support the SAR community and for overall Maritime Domain Awareness. The SAROPS system provides a specialized geographic display built upon the C/JMTK based Mapping Framework (i.e., tailored ESRI ArcMap), specialized software modules (i.e., extensions) for search planning and numerous spatial databases.

SPONSOR:
US Coast Guard

LOCATIONS:
NSWC Dahlgren

PARTNERS:
IT 5.18





ASSESSMENT RESULTS:
SAROPS operated on the HS/HD domain and received a Warfighter, Technical/ Interoperability and Information Assurance assessment.

SAROPS successfully demonstrated Objective 2.

- Used complex simulation techniques and algorithms to generate optimal search and rescue patterns remotely through servers located in Martinsburg, VA.
- Generated search patterns using current environmental and weather data through the USCG enhanced Mobile Incident Command Post (eMICP) at Dahlgren, VA.
- SAROPS search pattern and products shared between DoD, Coalition partners, local law enforcement, and first responders.
- SAROPS technology successfully integrated into the CWID network via the Local Area Network and Satellite tachyon link in the eMICP.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.24
Hybrid Multilevel Environment

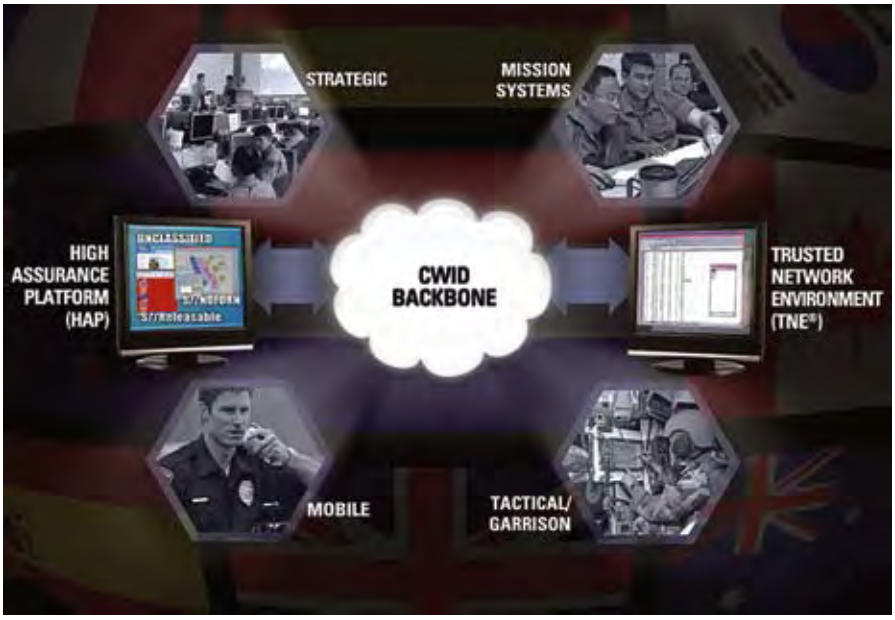
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: HME leverages and combines the Multiple Independent Levels of Security (MILS) and Multilevel Security (MLS) capabilities of High Assurance Platforms (HAP) and Trusted Network Environments (TNE) into a hybrid multilevel environment. HMI also provides an MLS datastore (data labeling, data access control, converged applications, networks and datastore) and a multi-level access client (converged networks and data access). Together, the MILS and MLS technologies allow dynamic access, creation, management, and removal of Communities of Interest (COIs). HME incorporates a converged network topology using NSA Type 1 encryptors for bulk encryption and commercial off-the-shelf (COTS) Inernet Protocol Security (IPSec) VPN devices for COI separation.

SPONSOR:
DISA

LOCATIONS:
NSWC Dahlgren

PARTNERS:
None



ASSESSMEMT RESULTS:
The HME Trial operated on the CTF domain and received a Warfighter, Technical/Interoperability and Information Assurance (IA) assessment.

HME successfully met Objective 2.

■ Demonstrated five categories of a Defense Information System Agency (DISA) Request for Proposal (RFP) and Statement of Work (SOW) supporting the Combined Enterprise Regional Information Exchange System (CENTRIX) Cross Enclave Requirement (CCER) project. These requirements covered five categories; (1) Technology concepts for Data Labeling and Tagging, (2) Technology concepts for Data Access Control, (3) Technology concepts for Converged Applications, (4) Technology Concepts for Converged Networks, and (5) Technology Concepts for Converged Data Storage.

■ Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.26
Stealth Solutions for Networks

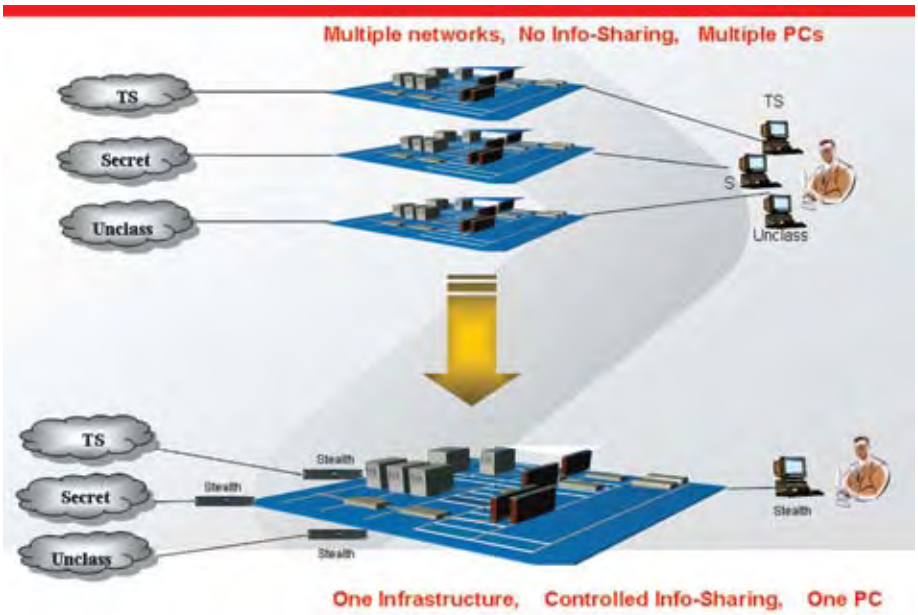
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: Stealth addresses the Converging Networks capability for the Combined Enterprise Regional Information Exchange System (CENTRIXS) Cross Enclave Requirement (CCER). Stealth converges multiple networks, creating virtual communities of interest (COIs) that can co-exist on a single infrastructure, while controlling access to COI information based upon defined user roles. COIs can share a common infrastructure, while remaining isolated from each other and allowing access by authorized users to COI data. Stealth offers unprecedented security for data in motion. Stealth is currently FIPS 140-2 certified for Secure but Unclassified (SBU) data. With EAL-4+ certification, it will permit data classified at different security levels to co-exist on a single physical infrastructure.

SPONSOR:
DISA

LOCATIONS:
NSWC Dahlgren
ESC Hanscom

PARTNERS:
None



ASSESSMEMT RESULTS:
The Stealth Trial operated on the CTF domain and received a Technical/Interoperability and Information Assurance (IA) assessment.

Stealth successfully met Objective 2.

■ Demonstrated one of the five categories of a Defense Information System Agency (DISA) Request for Proposal (RFP) and Statement of Work (SOW) supporting the Combined Enterprise Regional Information Exchange System (CENTRIX) Cross Enclave Requirement (CCER) project. The requirement was category 4, Technology Concepts for Converged Networks.

■ Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.27
Compartmented High Assurance Information Network

2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: CHAIN, a solution not a product, provides a framework for information sharing. CHAIN provides a windows-based solution for secure coalition interoperability, a Microsoft Windows-centric SOA (Service Oriented Architecture) for highly scalable interoperability with non-Windows platforms, and a CENTRIXS Cross-Enclave Requirement. CHAIN provides email, collaboration, web access, text chat, file sharing, and compartmented voice. Additionally, it provides information security, encryption, digital signatures, and content scanning. It satisfies fewer infrastructures, requires fewer people, allows better communication and needs less training. CHAIN's security features enhance information sharing, reduces unauthorized information, and simplifies sharing information with peers of different authorizations.

SPONSOR:
DISA

LOCATIONS:
USEUCOM

PARTNERS:
None

ASSESSMENT RESULTS::
The CHAIN Trial operated on the CTF domain and received a Warfighter, Technical/ Interoperability, and Information Assurance (IA) assessment.

CHAIN successfully demonstrated Objective 2.

■ Demonstrated five categories of a Defense Information System Agency (DISA) Request for Proposal (RFP) and Statement of Work (SOW) supporting the Combined Enterprise Regional Information Exchange System (CENTRIX) Cross Enclave Requirement (CCER) project. These requirements covered: (1) Technology concepts for Data Labeling and Tagging, (2) Technology concepts for Data Access Control, (3) Technology concepts for Converged Applications, (4) Technology concepts for Converged Networks, and (5) Technology concepts for Converged Data Storage.

■ Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.28
Secure Information Sharing Architecture

2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: SISA provides coalition warfighters a commercial off-the-shelf (COTS) solution for secure information sharing. SISA is created to house multiple communities of Interest (COI's) in a single consolidated environment. The tenets of the architecture include access protection, management and controls for authenticated access to networks, client, and server endpoints, content protection, collaboration services with persistent protection against inadvertent or malicious disclosure of files, documents, and e-mails. SISA provides data protection, management, encryption, continuity, scalability, and separation to protect stored data from external and internal threats, adaptive threat Defense, and intelligent auditing and intrusion detection.

SPONSOR:
DISA

LOCATIONS:
ESC Hanscom

PARTNERS:
None

ASSESSMENT RESULTS:
The SISA Trial operated on the HS/HD domain and received Warfighter, Technical/ Interoperability, and Information Assurance (IA) assessment.

SISA successfully demonstrated Objective 2.

■ Demonstrated one of the five categories of a Defense Information System Agency (DISA) Request for Proposal (RFP) and Statement of Work (SOW) supporting the Combined Enterprise Regional Information Exchange System (CENTRIX) Cross Enclave Requirement (CCER) project. The requirements covered category (1) Technology concepts for Data Labeling and Tagging, and (2) Technology concepts for Data Access Control

■ Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.29
Federated Identity Management System

2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

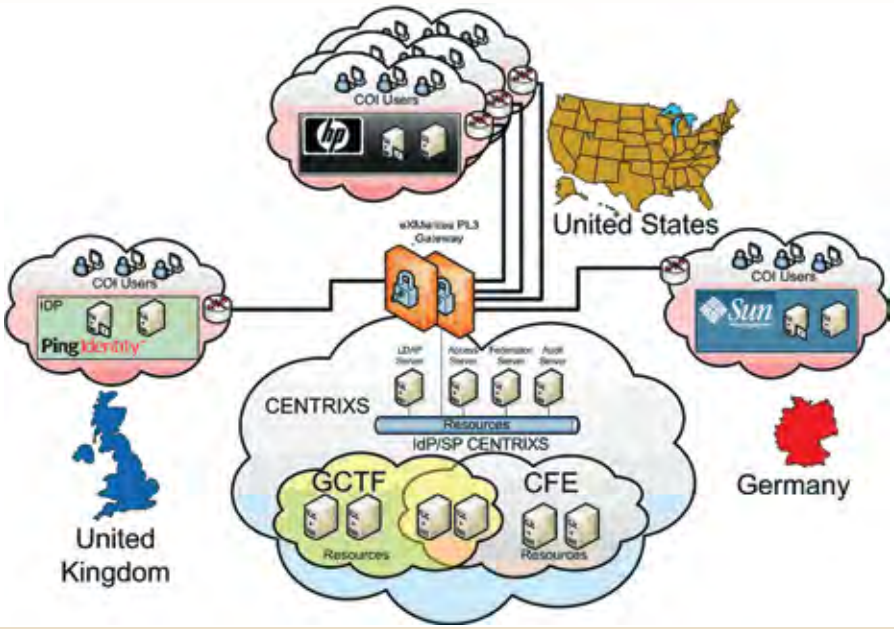
TRIAL OVERVIEW: FIdM shares information across Communities of Interest (COI) effectively and securely. The solution integrates various commercially available identity and access management products to provide cross-enclave access control. FIdM addresses the data access control capability for Combined Enterprise Regional Information Exchange System (CENTRIXS) Cross Enclave Requirement (CCER). The FIdM solution allows users to authenticate in their home domain to their local identity provider, pass identity attributes and roles to a remote COI, eliminate separate accounts to reduce user management costs and provide single sign-on, allow information providers to create their own access control policies, and maximize re-use of existing infrastructure investment.

SPONSOR:
DISA

LOCATIONS:

SPAWAR

PARTNERS:
None



ASSESSMEMT RESULTS:
The FIdM Trial operated on the CTF domain and received a Warfighter, Technical/ Interoperability and Information Assurance (IA) assessment.

FIdM successfully met Objective 2.

- Demonstrated one of the five categories of a Defense Information System Agency (DISA) Request for Proposal (RFP) and Statement of Work (SOW) supporting the Combined Enterprise Regional Information Exchange System (CENTRIX) Cross Enclave Requirement (CCER) project. The requirement covered was category (2) - Technology Concepts for Data Access Control.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.46
Information Integration Dashboard for Mission Support Planning

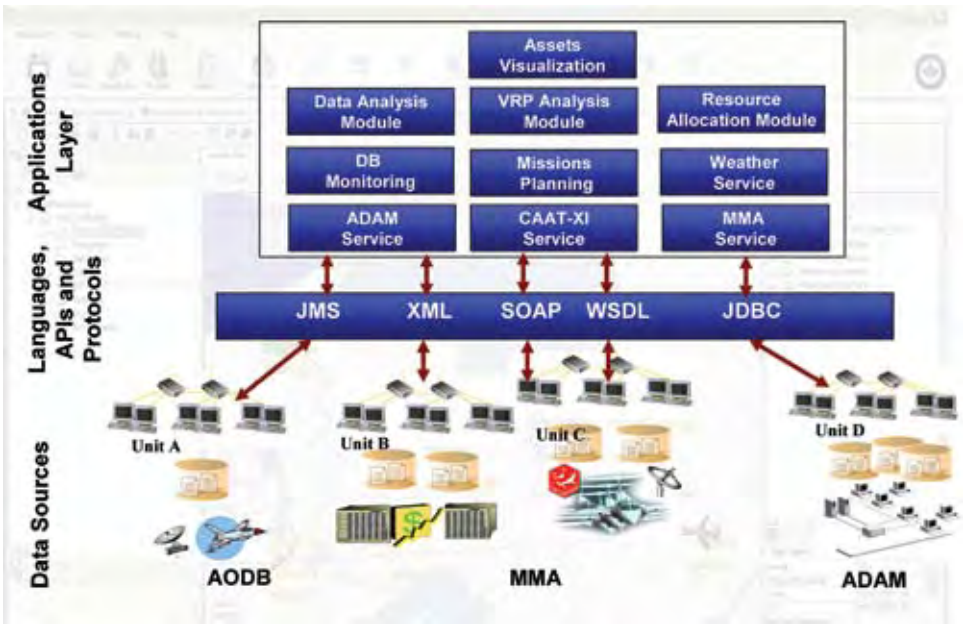
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: IID is a middleware based network centric environment for information/data integration. This decision support system is a multi-layer IT platform that provides a plethora of services such as data and service integration, monitoring, analysis and process optimization. The platform uses advanced display mechanisms to render structured information and provide navigational representation to drill down into details. IID integrates existing military distributed sources of information, wraps existing applications to turn them into modern web services, integrates and composes web services according to adequate business processes in order to propose new relevant and useful services, and leverages web services for asset visualization and distributed continual planning purposes.

SPONSOR:
Canada

LOCATIONS:
ESC Hanscom
Canada
NATO

PARTNERS:
None



ASSESSMEMT RESULTS:
The IID Trial operated on the CTF domain and received a Warfighter and Technical/ Interoperability assessment.

IID successfully met Objective 2.

- Demonstrated secure web-based access to the Dashboard using Service Oriented Architecture procedures.
- Demonstrated complementary planning tools that supported coalition planning activities enabling faster decision-making.
- Demonstrated information sharing by providing real time data (flight pattern, fuel, crew, and airports) to data bases and authorized users.
- Demonstrated ability to review aircraft inventory parts, and other logistical data.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.80
Thin Sessions

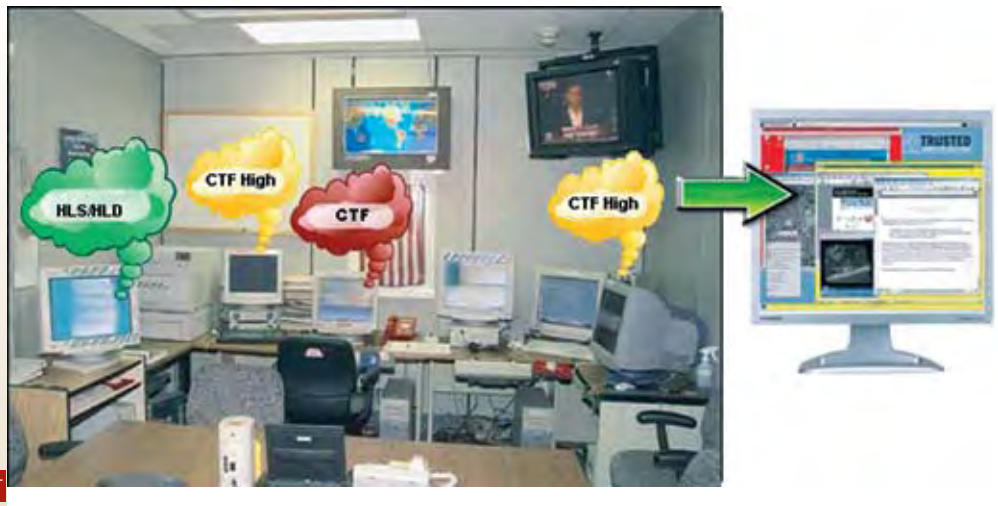
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: ThinSessions, a Protection Level 4 (PL4) accredited/Evaluation Assurance Level 4 Plus (EAL4+) certified, Multi-Level Security (MLS) Desktop Environment, establishes a virtualized computing session between distinct classification domains from a single user appliance. The technology allows simultaneous desktop access to multiple security levels using a single Thin Client Appliance and permits access to Windows® and UNIX® applications for office automation, email, web browsing, and collaboration. TS decreases hardware, maintenance, and infrastructure costs. Built on a trusted Linux system, TS demonstrates requirements with cross-domain solutions and when coupled with the Trusted Gateway, data can be transferred from one security domain or network to both lower and higher classified domains.

SPONSOR:
US Joint Staff

LOCATIONS:
USEUCOM
NSWC Dahlgren
SPAWAR
Canada
NATO

PARTNERS:
None



ASSESSMEMT RESULTS:
The TS Trial operated on the CTF domain and received a Technical/ Interoperability and Information Assurance (IA) assessment.

TS marginally successfully demonstrated Objective 2.

■ Due to unresolved integration issues, TS failed to execute the majority of planned events.

■ Established a Multi-level Security (MLS) Desktop Environment at SPAWAR with devices that created a computing session between distinct classification domains from a single user appliance with security controls.

■ Documented transfer from CTF HIGH to CTF. The system performed dirty word searches and virus scans. Document reviews included human interface.

■ Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.82
Proximity-Sensitive Session-Support Services

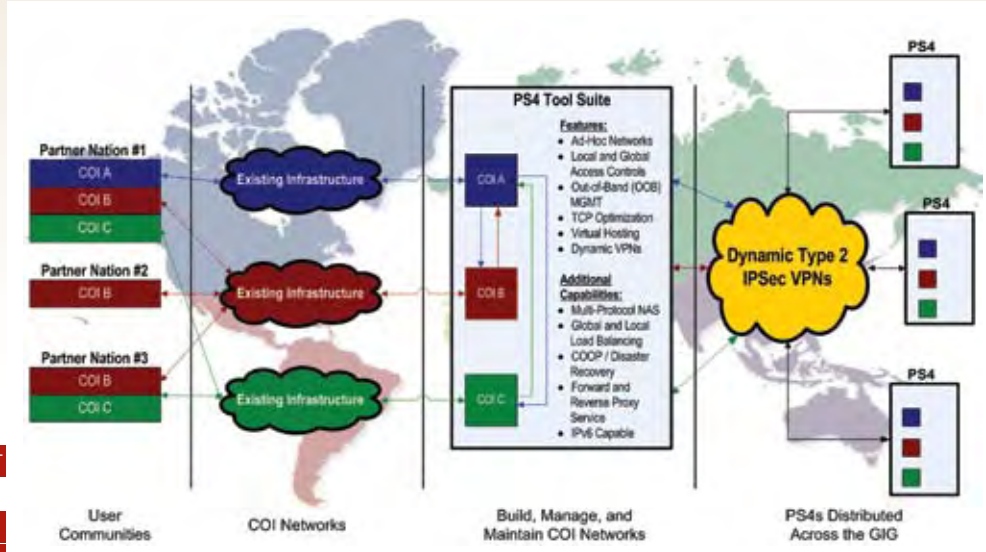
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: The Proximity-Sensitive Session-Support Services (PS4) addresses a Converging Network, leverages existing infrastructure and provides transparent, discretely separated Communities of Interest (COI) without user interaction, using existing transport. The technology supports central management by integrating with existing JTF-GNO central management and provides local and global COI separation by enabling COI boundaries by central administrators and varying access controls. PS4 builds dynamic, type 2, VPN tunnels and establishes end-to-end connectivity without relying on VPN concentrators. PS4 integrates COTS products and features a product suite that uses common criteria and complies with FIPS 140-2 while optimizing TCP and improving high-latency, low-bandwidth environments.

SPONSOR:
DISA

LOCATIONS:
ESC Hanscom

PARTNERS:
None



ASSESSMEMT RESULTS:
The PS4 Trial operated on the CTF domain and received a Technical/ Interoperability and Information Assurance (IA) assessment.

PS4 successfully demonstrated Objective 2.

■ Demonstrated one of five categories of a Defense Information System Agency (DISA) Request for Proposal (RFP) and Statement of Work (SOW) supporting the Combined Enterprise Regional Information Exchange System (CENTRIX) Cross Enclave Requirement (CCER) project. The requirement was category (4) -Technology Concepts for Converged Networks.

■ Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.83
Agile Coalition Environment

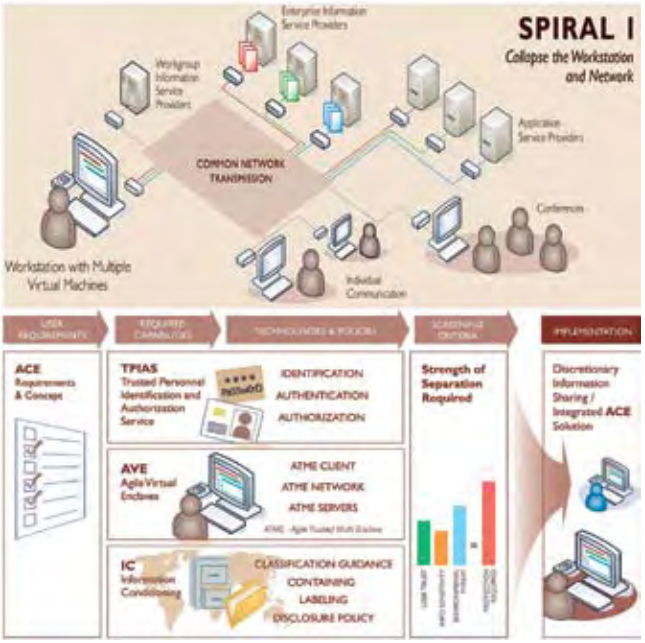
2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: ACE is a National Security Agency (NSA) supported U.S. Pacific Command initiative designed to address DISA's Combined Enterprise Regional Information Exchange System (CENTRIXS) Cross Enclave Requirement (CCER) for Collapsed Networks. The ACE architecture provides a foundation for secure and agile enclave instantiation and cross domain access. ACE is an evolving solution set that offers systems and capabilities through a spiral development, accreditation, and deployment process. The ACE virtual client workstation and collapsed network architecture are featured for the CWID 2008 demonstration.

SPONSOR:
DISA

LOCATIONS:
SPAWAR

PARTNERS:
None



ASSESSMEMT RESULTS:
The ACE Trial operated on the CTF domain and received a Technical/ Interoperability and Information Assurance (IA) assessment.

ACE successfully met Objective 2.

■ Demonstrated one of the five categories of a Defense Information System Agency (DISA) Request for Proposal (RFP) and Statement of Work (SOW) supporting the Combined Enterprise Regional Information Exchange System (CENTRIX) Cross Enclave Requirement (CCER) project. The requirement was category (4) - Technology concepts for Converged Networks.

■ Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 2.84
Smart Data Flow

2. IMPROVE INFORMATION SHARING ACROSS THE FULL RANGE OF MILITARY OPERATIONS ●

TRIAL OVERVIEW: SDF is an Office of Naval Research (ONR) and U.S. Pacific Command initiative that addresses DISA's CENTRIXS Cross Enclave Requirement for managing services on converged networks in the enterprise coalition environment. SDF provides an intelligent network management solution for controlling and configuring network devices in real-time. This software application's extensive visualization capabilities improve network situational awareness and allow less seasoned operators to manage networks with reduced risk of error. SDF manages traffic load on converged, encrypted networks, resulting in reliable Quality of Service (QoS) in the dynamic multi-community of interest (COI) environment.

SPONSOR:
DISA

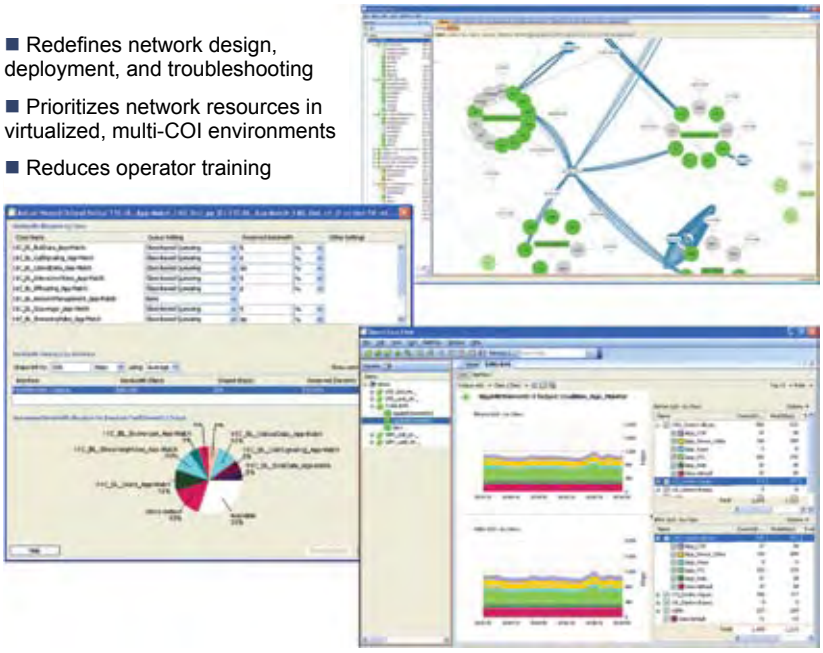
LOCATIONS:
SPAWAR

PARTNERS:
None

■ Redefines network design, deployment, and troubleshooting

■ Prioritizes network resources in virtualized, multi-COI environments

■ Reduces operator training



ASSESSMEMT RESULTS:
The SDF Trial operated on the CTF domain and received Technical/ Interoperability and Information Assurance (IA) assessment.

SDF successfully met Objective 2.

■ Demonstrated one of the five categories of a Defense Information System Agency (DISA) Request for Proposal (RFP) and Statement of Work (SOW) supporting the Combined Enterprise Regional Information Exchange System (CENTRIX) Cross Enclave Requirement (CCER) project. The requirement was category (4) -Technology concepts for Converged Networks. However, SDF only demonstrated two of the four requirements for that category.

■ Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 3.70

Coalition Dual Phenomenology Data Fusion - U.S.

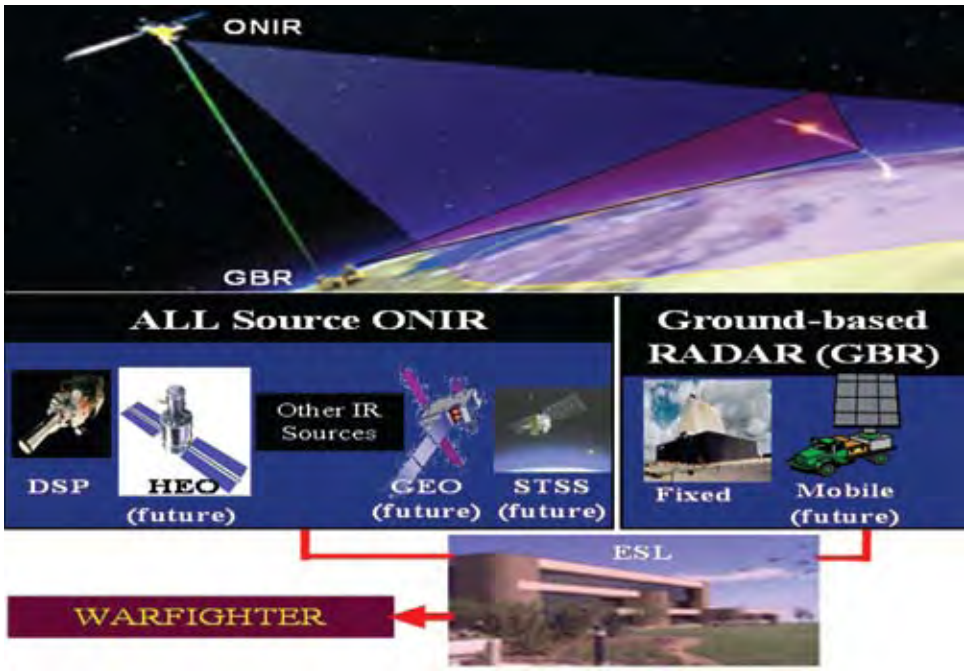
3. ENHANCE CROSS-DOMAIN AND MULTIPLE SECURITY LEVEL INFORMATION EXCHANGE TOOLS ●

TRIAL OVERVIEW: CDPDF targets the machine-to-machine fusion of two mutually complimentary sensors. Overhead Non-imaging Infra-red (ONIR) sensors are exceptional at geo-locating targets of interest, but their performance at determining velocity state vectors is sub-optimal. High frequency (HF) Ground-based RADAR (GBRs) have been used for decades, and offer improved velocity state vectors, but lack high fidelity geo-location. CDPDF fuses data from different sources yielding both location and vector information.

SPONSOR:
US AIR FORCE

LOCATIONS:
USEUCOM

PARTNERS:
None



ASSESSMEMT RESULTS:
The CDPDF-US Trial operated on the CTF domain and received a Warfighter and Technical/ Interoperability assessment.

CDPDF successfully demonstrated Objective 3.

- Demonstrated a visualization and integration tool that tracked Theater Ballistic Missile (TBM) from its launch location, through its flight path, and to the estimated impact point.
- Fused Overhead Non-Imaging Infrared (ONIR) sensors and High Frequency Ground-based RADAR (GBR), and sent data to GCCS-A as a TAB-37 formatted message.
- Allowed Senior leaders to generate timely defense actions and conducted countermeasures based on CDPDF-US fused data.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 5.06

Common Information Centric Security

5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: SecureD® provides data at rest encryption. Sponsored by the U.S. office of the Secretary of Defense, SecureD® is the product of a joint US-Norwegian project and has earned Common Criteria EAL4+ and FIPS 140-02 Level 3 certifications. Available in laptop, desktop, and USB portable disk drive versions, SecureD® offers real-time security that is transparent to users and independent from operating systems. SecureD® uses a 256-bit key inserted directly between the hard drive controller and hard disk drive, and can be authenticated via smart card token or radio token.

SPONSOR:
OSD

LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
SPAWAR
Canada

PARTNERS:
None

ASSESSMEMT RESULTS:
The SecureD Trial operated on the HS/HD domain and received a Warfighter and Information Assurance (IA) assessment and a SEIWG evaluation.

SecureD successfully met CWID Objective 5.

- Provided a ready to field Common Criteria EAL4+, FIPS 140-02 Level 3, and JITC certified hardware solution for encrypting DoD sensitive unclassified data at rest on Mobile and stationary computing devices and removable storage media.
- Supported laptops, desktops, and USB portable disk drives using smart card or radio tokens for security authentication.
- Provided warfighters a straightforward, easy to use, intuitive approach for protecting data.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 5.14

Battlespace Terrain Reasoning and Awareness - Battle Command Commercial Joint Mapping Toolkit (BTRA-BC CJMTK) Extensions

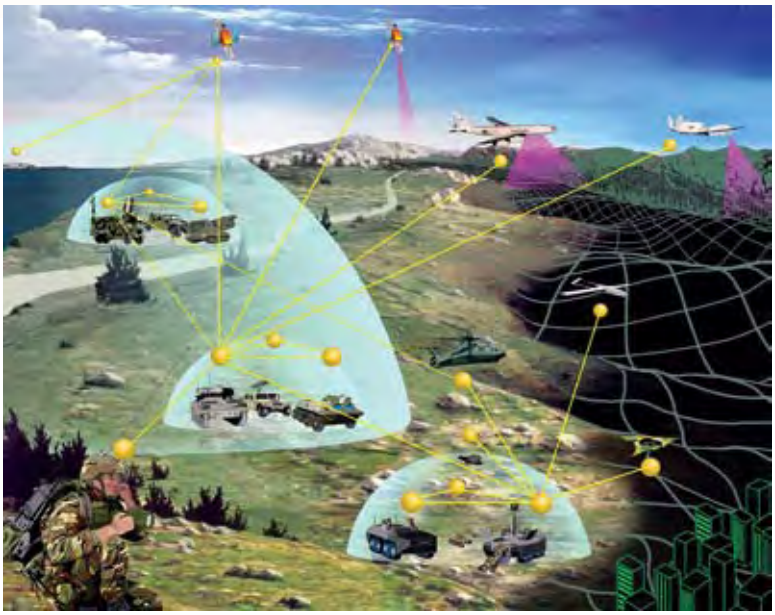
5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: The BTRA-BC CJMTK Extensions (BCE) project is a result of a technology transfer agreement arranged by the U.S. Army Topographic Engineer Center (TEC) and the National Geospatial-Intelligence Agency (NGA). The Battlespace Terrain Reasoning and Awareness - Battle Command (BTRA-BC) project at U.S. Army TEC creates advanced geospatial and terrain reasoning tools designed to enable the Military Decision Making Process (MDMP). The BCE project is tasked with transitioning the BTRA-BC engines to the C2I developer community via the Commercial Joint Mapping Toolkit (CJMTK) program.

SPONSOR:
US ARMY
NGA

LOCATIONS:
USEUCOM
NSWC Dahlgren
SPAWAR

PARTNERS:
None



ASSESSMEMT RESULTS:
The BTRA-BC CJMTK Extensions (BCE) Trial operated on the CTF domain and received a Warfighter, Technical/ Interoperability, and Information Assurance (IA) assessment.

BCE successfully met CWID Objective 5.

- Demonstrated situational awareness through effective terrain analysis, choke point identification and route planning which provided commanders an improved information sharing and collaborative planning capability.
- Generated terrain analysis and choke point analysis using JPEG and XML data from CJMTK Geospatial Appliance (CGA). Using the BCE Data Application and the CGA warfighters retrieved the required map and used the Movement Projection tool to determine Start, Way and Stop points for ingress and egress routes.
- Maintained an adequate IA security posture; some vulnerabilities and open ports/services noted for correction in future releases.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 5.18

enhanced Mobile Incident Command Post

5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: The eMICP is a 53 foot long trailer with office space, a conference room and a basic communications suite. The primary function of eMICP is to provide sheltered workspace, voice and data connectivity as well as Command and Control (C2) capabilities on a mobile platform. The eMICP also serves as a source of power and network infrastructure for portable MCC assets. It provides an environmentally protected work area to those using the command post and/or the robust communications equipment in the Mobile Communications Vehicle (MCV). When interfaced with the MCV, advanced communication capabilities are piped into the office space in the eMICP. It is deployable in the Continental United States (CONUS) by commercial tractors and supplies VHF and UHF radios that are interoperable with first response partners and other agencies.

SPONSOR:
US Coast Guard

LOCATIONS:
NSWC Dahlgren

PARTNERS:
IT 1.53
IT 1.79
IT 2.16
IT 2.17

ASSESSMEMT RESULTS:
The eMICP trial operated on the HS/HD domain and received a Warfighter, Technical/ Interoperability assessment and an Information Assurance (IA) assessment.

eMICP met Objective 5.

- Demonstrated a fully loaded multi-mission secure mobile operational Command and Control (C2) center for emergency and contingency operations.
- Provided a satellite link, communication and briefing suite, and a collaboration center that supported twenty two workstations with Voice over Internet Protocol and traditional telephone land lines.
- Demonstrated autonomy using a generator and satellite link.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 5.34

Poliwall with Heuristic Internet Protocol Packet Inspection Engine Appliance

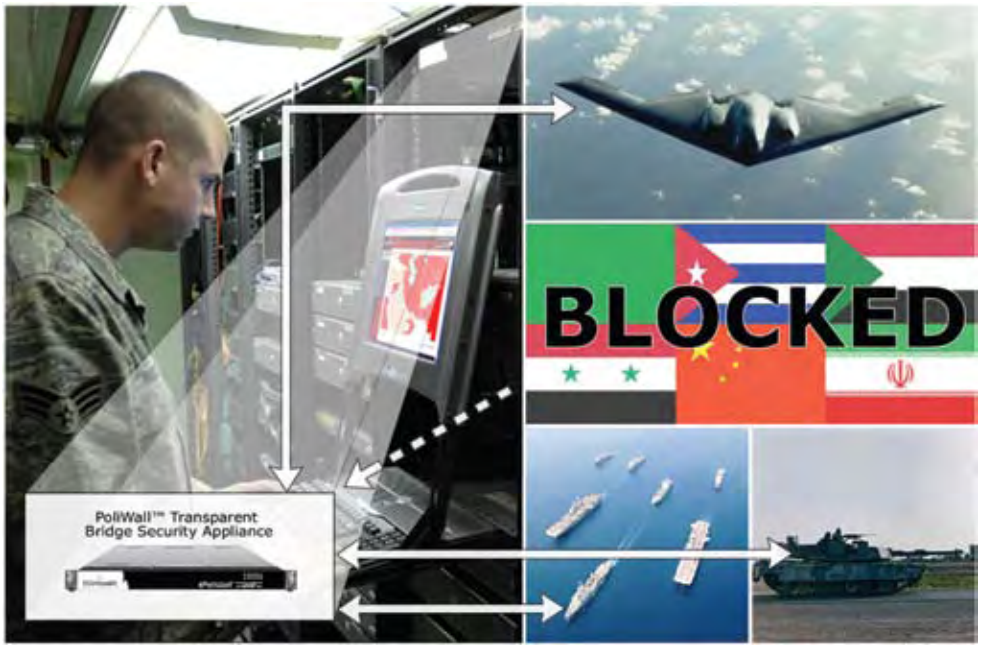
5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: PoliWall's HIPPIE Appliance blocks network traffic from adversary nations and gives U.S. and coalition partners higher priority to network assets. Security policies can be quickly configured using a simple and intuitive world-map based interface. PoliWall can be configured to detect changes in traffic patterns from nation-states and send alerts or automatically change configuration to apply more restrictive policies, mitigating the impact of hostile activity. Network visualization and reporting tools provide real-time and historical views of network used by nations.

SPONSOR:
DISA

LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom

PARTNERS:
IT 5.65



ASSESSMENT RESULTS:
The Poliwall with HIPPIE Trial operated on the HS/HD domain and received a Warfighter, Technical/ interoperability, and an Information Assurance (IA) assessment.

Poliwall with HIPPIE successfully demonstrated Objective 5.

- Demonstrated a graphical display of incoming network traffic by country and unique (in front of firewall) solution for the detection of Denial of Service attacks from single country or combination of countries.
- Using a graphical map interface allowed IA specialists to set network policies for blocking traffic
- Dramatically reduced the time to block or throttle internet bandwidth from individual and or groups of countries compared to traditional firewalls.
- Automatically sent alerts to appropriate staff and systems.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 5.48

Federated Intelligence Network

5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: The FedIntel network is designed to facilitate compliance with the National Response Framework (NRF) and the National Incident Management System (NIMS) and provides a common ground for vertical and horizontal information sharing and collaboration across local, state, federal, military and international domains. The emergency management extensions of FedIntel aid with preparedness, communication, information, resource, command management, and on-going maintenance. The extensions provide incident specific policies and procedures to provide the right information to the right persons at the right time. Built upon Microsoft's SharePoint 2007 portal system, the FedIntel network uses alerting, workflows, domain security, and advanced document management features to make available information when needed to support the coordination of resources and strategies in the field and to provide real-time reports up the chain of command.

SPONSOR:
USNORTHCOM

LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscome
Canada
Charleston, WV
Richmond VA
Smyna DE

PARTNERS:
None

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

ASSESSMENT RESULTS:
FedIntel operated on the HS/HD domain and received a Warfighter and Technical/Interoperability assessment.

FedIntel successfully demonstrated Objective 5.

- Provided a framework for all levels of government and non-government agencies to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents regardless of cause, size, location, or complexity.
- Provided a web-based solution increasing situational awareness and facilitating intelligence gathering activities to support incident response activities.
- Used an incident status dashboard that provided a high-level picture in real time of nation-wide occurrences.
- Provided interagency interoperability and collaboration capabilities ensuring consistent incident status at all levels of the incident response hierarchy.

IT 5.59
Coalition Dual Phenomenology Data Fusion - USNORTHCOM

5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: CDPDF targets the machine-to-machine fusion of two mutually complimentary sensors. Overhead Non-imaging Infra-red (ONIR) sensors geo-locate targets of interest, but their performance at determining velocity state vectors is suboptimal. High frequency (HF) GBRs offer improved velocity state vectors, but lack high fidelity geo-location. CDPDF fuses data from these two sources to yield both location and vector information with minimal uncertainty, and with a timeliness that is useful to the Warfighter in the strictly compressed battle space of a short range ballistic missile attack.

ASSESSMEMT RESULTS:
The CDPDF-USNORTHCOM withdrew during Execution and therefore was not assessed.

SPONSOR:
USNORTHCOM

LOCATIONS:
USEUCOM
USNORTHCOM

PARTNERS:
None

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 5.64
Trusted Enterprise Service Bus

5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: TESB and Tactical Service Bus (TSB) provide a secure C4ISR service oriented architecture (SOA) supporting Maritime Interdiction Operations (MIO) at the tactical edge of the GIG. Also provides network quality of service via high assurance components in disciplined service architecture. TESB balances need-to-know vs. need-to-share and prioritizes bit delivery via a trusted, dynamic, authorization policy engine. An "Architecturally net-ready" assessment, Certification & Accreditation, and COTS competitive models support rapid deployment and continuous incremental improvements.

ASSESSMEMT RESULTS:
TESB operated on the CTF domain and received a Warfighter, Technical/Interoperability and Information (IA) Assurance assessment.

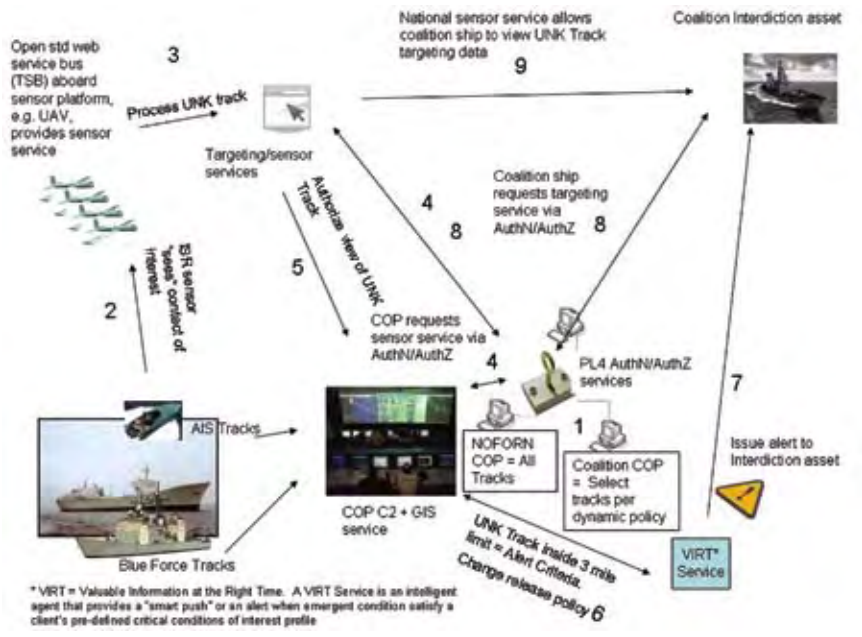
TESB successfully met Objective 5.

- Shared previously non-releasable data with coalition partners by setting security policies during normal, emergency and self-defense conditions that supported Maritime Domain Awareness.
- Users authenticated to an authorization engine which improved information assurance and security postures by data access, fusion and integration of AIS tracks, weather, geospatial, sensor and intelligent data within the CWID scenario.
- Changes in the security posture were transparent to the user in a need to know environment which aided collaboration between the end users.
- Maintained a good IA security posture. No vulnerabilities found.

SPONSOR:
NSA

LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
SPAWAR
ESC Hanscom
Canada
New Zealand

PARTNERS:
None



REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 5.65
Security Information Management for Enclave Networks

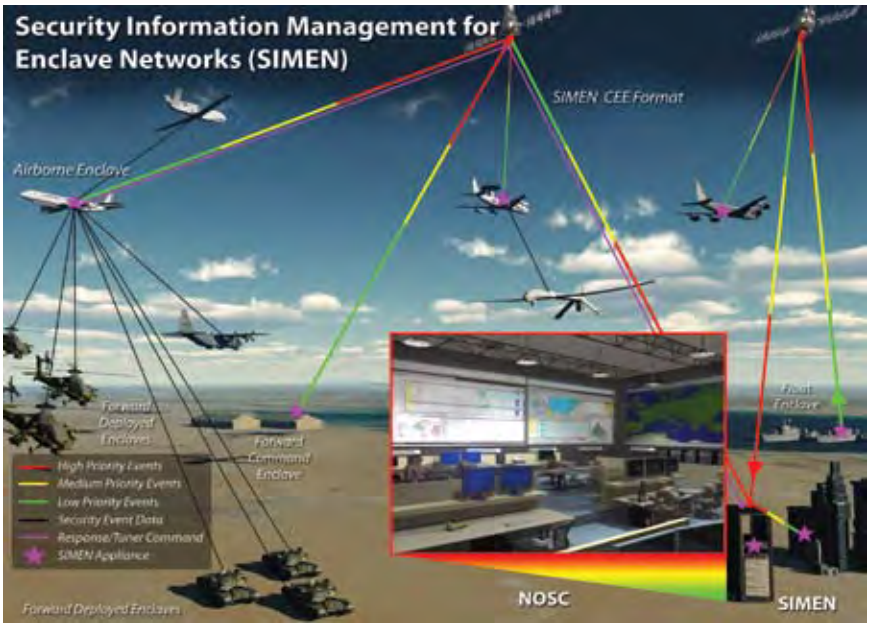
5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: SIMEN, a Global Information Grid (GIG) Information Assurance (IA) project, employs an enterprise-wide sensor grid that collects and feeds event messages to a centralized security monitoring location. Timely, threat focused collection and security event data processing is challenging with bandwidth constraints, high volumes of data, and rapidly evolving threat environments typical of tactical networks. SIMEN incorporates algorithms and protocols for the distributed collection and transport of IA events to a central location. SIMEN uses protocols and adaptive algorithms to dynamically respond to evolving threat environments, respect bandwidth constraints, prioritize events, and minimize fluctuating event volumes.

SPONSOR:
US Air Force

LOCATIONS:
USNORTHCOM
NSWC Dahlgren
ESC Hanscom

PARTNERS:
IT 2.01
IT 5.34



ASSESSMEMT RESULTS:
SIMEN operated on the HS/HD domain and received a Warfighter, Technical/Interoperability, and Information Assurance (IA) assessment.

SIMEN successfully demonstrated Objective 5.

- Filtered event messages at the collection point, threat prioritizing the remaining critical messages, and then reducing the filtered, prioritized messages in actual size before sending to the monitoring center.
- Accepted network security event messages from a commercial network security product and correctly prioritized and processed the messages based on threat level.
- Provided remote reach back to change the threat focus of its enclave collection device to quickly identify a developing network threat from a hostile country.
- Maintained a good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 5.73
VirtualAgility OPS Center

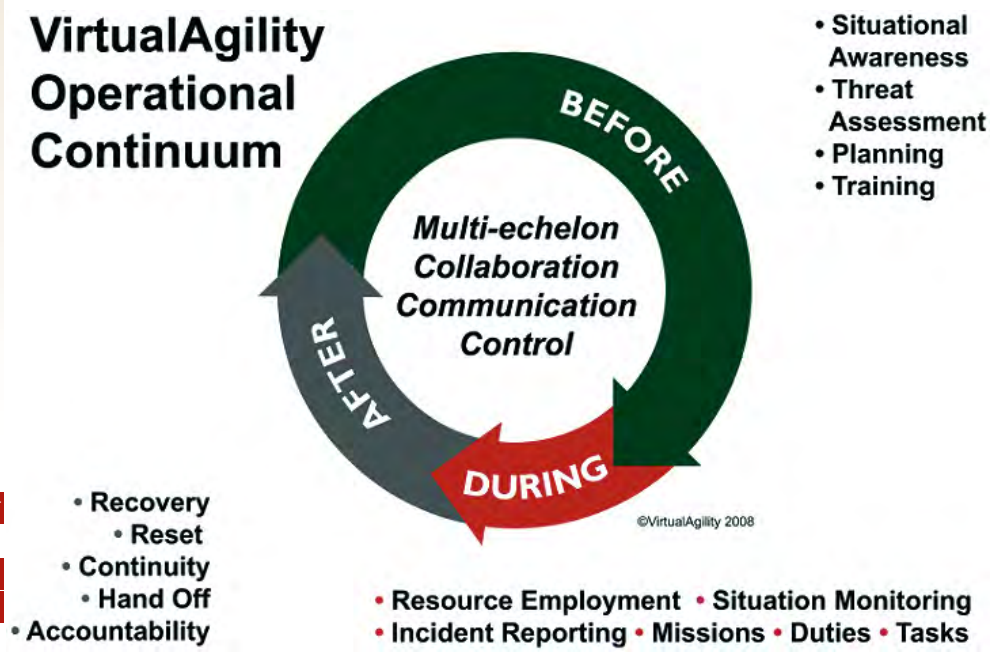
5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: VOC addresses the entire crisis management continuum – before, during and after an event. VOC is a solution that provides operational decision support in real time enabling multiple public and private organizations to collaborate and communicate in a single, centralized environment to plan, train, organize, track and share information and enable dynamic response to changing conditions. The VirtualAgility OPS Center (VOC) is a service-oriented architecture environment that allows multiple organizations using different technologies to plan, share, respond and recover with unprecedented levels of coordination, integration, accountability, and real-time situational awareness.

SPONSOR:
Canada

LOCATIONS:
USNORTHCOM
NSWC Dahlgren
SPAWAR
Canada
Richmond, VA

PARTNERS:
None



ASSESSMEMT RESULTS:
VOC operated on the HS/HD domain and received a Warfighter assessment and SEIWG evaluation.

VOC successfully demonstrated Objective 5.

- Provided role-based, service-oriented architecture that enabled interoperability and collaboration for multiple agencies to perform crisis, enhancing government agency interoperability.
- Used the National Response Framework (NRF) for creating new plans in response to a crisis.
- Warfighters found the trial intuitive, allowing quick access to the multi-agency collaborative data for situational awareness, identifying critical risks and impacts, discovering and mapping critical infrastructure, and for coordinating track response efforts by government agencies and first responders.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

IT 5.81
Transnational Information Sharing Coalition

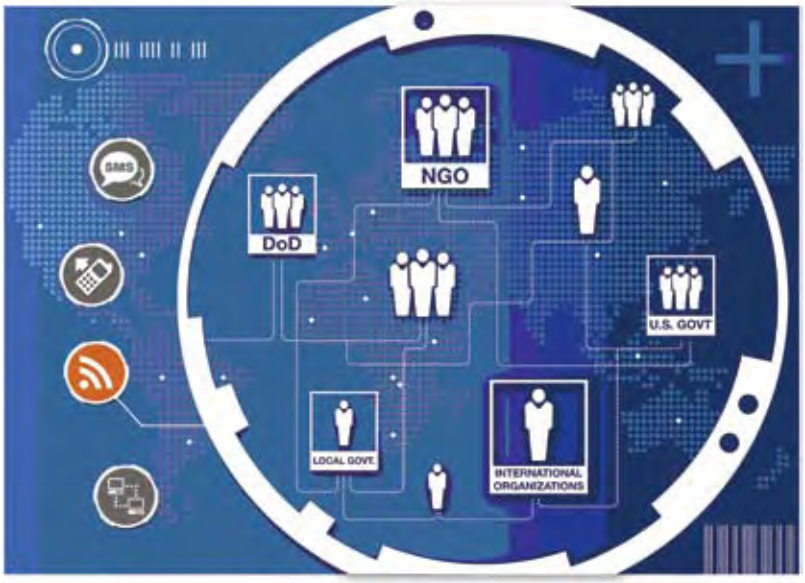
5. ENHANCE GOVERNMENT AGENCY INTEROPERABILITY ●

TRIAL OVERVIEW: TISC represents a radical departure from existing information sharing approaches by driving collaboration towards the web. TISC engages a range of open source communities to create an outward-facing collaborative network based on web-native architecture. The complexity of multi-organizational stability, security, transition and reconstruction (SSTR) environments and the rising need to cooperate across institutional boundaries are addressed by offering collaborative technologies that facilitate informational exchanges while preserving organizational integrity. Open technology development (OTD) based on standard protocols allows for immediate adoption by multiple organizations at significantly reduced cost of acquisition, thereby streamlining communications and allowing greater attention to be dedicated to core competencies.

SPONSOR:
USEUCOM

LOCATIONS:
USEUCOM
USNORTHCOM
NSWC Dahlgren
NATO

PARTNERS:
None



ASSESSMEMT RESULTS:
TISC operated on the HS/HD domain and received a Warfighter, Technical Interoperability, and Information Assurance (IA) assessment.

TISC successfully demonstrated Objective 5.

- Posted policy documents and reports to the TISC web-based portal for collaboration and information sharing between government agencies and first responders.
- Accessed the Preplanned Response Emergency Action Tool (PREACT) to determine the population affected by natural disasters (e.g. earthquake, flooding) and posting results to the TISC portal.
- Provided a multi-lingual chat feature in a variety of languages (e.g. English, Spanish, French) which enhanced the ability to collaborate with coalition forces.
- Maintained good IA security posture. No vulnerabilities found.

REPORT LINKS
FULL TRIAL REPORT
BRIEFS LINKS
TRIAL CONTENTS
CWID SUCCESSES

HISTORY OF CWID

CWID traces more than 17 years of history to establishment of the Secure Tactical Data Network (STDN) series originated by the U.S. Army to demonstrate emerging command, control, communications and computer (C4) capabilities.

STDN 1 and 2 concentrated on Army-only issues while STDN 3 brought the first multi-service participation. The Joint Staff recognized that advances in communications and information technology in the public sector were outpacing Department of Defense (DoD) capabilities.

The Joint Staff assumed sponsorship of the STDN series in 1993 under the C4I for the Warrior concept. The Defense Information Systems Agency (DISA) was directed to be Executive Agent, in concert with a lead Service, to organize network experiments, bringing emerging public sector and other government agency technologies into DoD projects and into war-fighters' sphere of recognition. DISA was also directed to improve joint C4 interoperability.

In 1994, annual STDN efforts evolved into the first Joint Warrior Interoperability Demonstration (JWID). The Air Force was lead service and U.S. Atlantic Command was host combatant command. The idea of moving from a static, one-dimensional picture of the battlefield to a near real-time, multi-dimensional battlespace picture became reality to joint and combined warfighters.

Key efforts in JWID '94 included demonstration of baseline segments of what became the Global Command and Control System (GCCS). Six weeks after the conclusion of JWID '94, GCCS was operationally deployed to U.S. Atlantic Command supporting military operations in Haiti. Full operational deployment of GCCS to all combatant commanders occurred within 12 months after JWID '94.

In 1997, the Chairman of the Joint Chiefs of Staff mandated interoperability in Joint Vision 2010, envisioning future conflicts as coalition operations. JWID assisted that vision, establishing itself as a coalition interoperability forum through invitations to Combined Communications Electronics Board (CCEB) nations (Australia, Canada, New Zealand and the United Kingdom) and NATO beginning with JWID '94 and continuing to the present. While invited participants used JWID to perform their own technology demonstrations and joint interoperability trials, their main intent was to promote and ensure C4 interoperability with the U.S.

EXPANSION

In 1998, JWID evolved into a two-year process to pursue selection and limited fielding of C4 technologies to warfighting combatant commanders. The Theme (first) Year conducted demonstrations and interoperability trials and selected "Gold Nuggets" for support and continued improvement during the Exploitation (second) Year, with eventual fielding to combatant commands. JWID '98 fielded three Gold Nuggets to warfighters.

U.S. Y2K concerns drove JWID '99-R to focus only upon coalition interoperability trials between the U.S. and CCEB/NATO nations. To more easily promote trials and other Command, Control, Communications, Computers and Intelligence (C4I) experiments, the Coalition Wide Area Network (CWAN), established annually for JWID, evolved into the standing Combined Federated Battle Laboratories Network (CFBLNet). The network permits C4I experimentation among the U.S. and nations of CCEB/NATO year-round, using systems jointly owned and managed by CFBL membership.

JWID '00-'01 restored the two-year cycle, with 23 U.S. demonstrations and 145 combined/coalition demonstrations worldwide. Two Gold Nuggets were fielded in 2001. In addition, a Distributed Collaborative Tool Set (DCTS, now Defense Collaboration Tool Suite) was refined and subsequently selected for worldwide fielding to the Unified Commands. DISA fielded the capability, within 72 hours, in support of the Office of the Secretary of Defense (OSD) requirements following terrorist attacks of September 11th, to multiple DoD networks.

COALITION INTEROPERABILITY

JWID 2002 featured transition from a limited fielding of technology to full focus on coalition interoperability, led by U.S. Pacific Command (USPACOM), the host combatant command. The demonstration included Pacific Rim nations in a Pacific Theater Initiative (PTI), with Japan, South Korea, Singapore, and Thailand participating while Malaysia and the Philippines observed operations. Coalition partners were integrated on the Multinational Task Force (MTF) and component staffs to maximize opportunities. The JWID CWAN continued use of CFBLNet architecture and services established in past demonstrations. U.S. Joint Forces Command (USJFCOM) fielded a JWID demonstrated language translation device.

JWID 2003 took coalition interoperability to new heights. USPACOM guided the CTF and, for the first time, Japan, South Korea, Thailand and Singapore provided staffing to expand information exchange over dual domains. One key focus for 2003 included management of information exchange between the traditional 6-eyes network to a larger, more robust 10-eyes network. The larger network was vital to JWID's success because Pacific Rim nations needed effective information to serve in MTF staff positions. JWID 2003 addressed multi-level security technical solutions and refinement of coalition policies and procedures to overcome issues surrounding information exchange.

DISA assumed duties as the lead agency, providing broad-base management support of JWID activities. Four Coalition Interoperability Trials (CITs) with especially noteworthy performance were submitted to USJFCOM J861, for consideration for limited fielding.

HOMELAND SECURITY

JWID 2004 featured U.S. Northern Command (USNORTHCOM) as the host combatant command. USNORTHCOM brought a Homeland Security/Homeland Defense (HS/HD) focus to the demonstration, breaking new ground beyond the traditional JWID coalition interoperability area. USNORTHCOM invited agencies within the Department of Homeland Security, including first-time participation for the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), the U.S. Coast Guard, and the National Guard Bureau. Limited coalition participation among these organizations occurred as Public Safety and Emergency management Canada (PCEPC) joined in the interoperability trials, beginning significant potential for more extensive cooperation among other coalition homeland security organizations and their U.S. counterparts. USJFCOM filled an ancillary role, assisting with select fielding of technologies to combatant commanders. JWID 2004 involved 25 countries, military services, and government agencies participating in a scripted scenario over a global network.

USNORTHCOM was host Combatant Command in 2005 as the demonstration moved forward with a name change. Now the Coalition Warrior Interoperability Demonstration (CWID), the shift from "Joint" to "Coalition" describes the larger community of participants, including national and international government agencies.

USJFCOM formally assumed oversight for planning and execution of CWID 2005 from the Joint Staff in July 2004. This involvement brings USJFCOM advocacy for U.S. combatant command interoperability shortfall resolutions to the forefront. USJFCOM's objectives included (1) to ensure CWID demonstrates relevant technologies that address combatant commander's capability gaps, (2) to investigate military, coalition and interoperability solutions and (3) to identify technologies suitable for prototype initiatives.

Fifteen trials were considered "success stories," moving forward for continued development. Seven ITs were selected for Service, Agency, or limited Combatant Commander fielding (including fielding in support of Hurricane Katrina). Two ITs achieved milestones and continue spiral development as Programs of Record. One was selected for funding via a Congressional Plus-up for further research and development, and one was submitted as a Limited Acquisition Authority candidate. Four others were identified for agency fielding in some capacity.

THE LARGER COALITION

U.S. European Command (USEUCOM) assumed host combatant command for 2006 through 2008. USNORTHCOM continued as the lead for HS/HD CWID operations.

Out of 34 trials in CWID 2006, USJFCOM published 12 U.S. and three coalition trials with potential to answer combatant-commander defined objectives. Four promising technologies were sponsored by USNORTHCOM.

The HS/HD site orchestrated a first live exercise associated with CWID, involving local Colorado Springs first responders. The Marine Corps and Army site, Dahlgren, Va., linked that portion of the scenario into Coalition Task Force operations over the CWID network.

USEUCOM coalition participants drove development of a multi-tier network to access HS/HD networks while still operating in the Coalition Task Force military scenario. Canada and USEUCOM joined the HS/HD enclave to fully participate in trial test and evaluation.

NATO used CWID 2006 to advance Transformation within the Alliance. The NATO Response Force (NRF), designed to be agile, joint and expeditionary, participated as a Coalition entity in the scenario for the first time. CWID provided a network to explore a robust and flexible Computer Information Systems (CIS) environment, key to the NRF concept.

CWID 2007 evaluated 47 trials. Twelve of those were noted as promising technologies for U.S. forces with five additional Coalition-sponsored trials of note for possible fielding.

2007 was the first year a concerted effort was made to involve programs of record, utilizing the CWID protected network and scripted scenario for risk reduction in the DoD acquisition cycle.

USJFCOM J-8, Joint Capability Development Directorate, assumes combatant command leadership for 2009 and 2010. USEUCOM will retain its role as U.S. lead to United Kingdom and NATO CWID. USJFCOIM intends to continue focused support for technologies already in acquisition channels as well as new and emerging commercial sector efforts.

CWID Heritage of Delivering Successful Warfighting Solutions

CWID trials are assessed for warfighter utility, technical interoperability and information assurance. Fortyone Innovative solutions demonstrated between 1994 and 2007 are listed here by generalized objectives. Technologies here are in operational use today as evolved versions of interoperability trials, components of tool suites, and/or deployed as originally demonstrated in CWID.

GENERAL OBJECTIVE:

Improve coalition and joint command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) architecture

■ **Global Command and Control System (GCCS)** Fielded system in support of Haiti operations; provided to all combatant commands within 12 months of demonstration

■ **Expand Networks Data Accelerator** Increased bandwidth over wide area networks (WANs); fielded with U.S. Navy and allied naval forces for data transmission links

■ **Coalition Warfare Program (CWP)**: Scalable, network-centric computing capability employing "smart card" technology; considered precursor to DoD Common Access Card

■ **Blue Force Tracking (BFT):** Initial demonstration of Coalition BFT situational awareness capability; used near-real time Global Positioning System (GPS) precision tracking to enhance visibility of friendly forces; reduces fratricide today as component of C2 suites

■ **Global Personnel Recovery System (GPRS):** U.S. Air Force sponsored; developing capability that provides worldwide, over-the-horizon tracking, locating and two-way text messaging to complement existing GPS utilities

■ **Tactical Emergency Asset Management System (T.E.A.M.)**: North American Aerospace Defense-U.S. Northern Command (NORAD-USNORTHCOM) sponsored; fielded to provide a small-footprint, self-deployable system for net-centric, mobile, interoperable communications for emergency response

■ **Weapons of Mass Destruction Collaborative Advisory Response System (WMD CARS):** NORAD-USNORTHCOM sponsored; on-scene commander's collaborative web-based portal for critical WMD and chemical, biological, radiological and nuclear (CBRN) response

■ **Enhanced Video, Text and Audio Processing (eVITAP):** First fully automated, commercially available real-time foreign media analysis, multi-lingual, broadcast news monitoring capability; searchable, real-time data for rapid analysis

■ **MobiKey Identity Based Access Drive and Defense Identity Management Network (MobiKey IBAD and DEFIMNET):** Canadian sponsored; U.S. Navy Reserve pilot program; flexible, convenient and user-friendly crypto device for remote access to home network computing resources using standard "USB Port" device for password and digital certificates.

GENERAL OBJECTIVE:

Information sharing across the full range of civil and military operations

■ **Compartmented High Assurance Information Network (CHAIN)**: NORAD-USNORTHCOM sponsored framework for information sharing

■ **Coalition Portal for Imagery and Geospatial Services (CPIGS):** Fielded; providing operational geospatial-Intelligence support to U.S. Army Airborne forces

■ **Defense Message System (DMS):** Meets DoD requirements for secure, accountable, writer-to-reader messaging; explored capability to extend Simple Message Transfer Protocol messages to allies in a coalition environment

■ **Language Translation Services:** Instant message format devices procured for combatant command's machine-to-machine language translation

■ **Bi-Directional Korean Machine Translation Tool Suite:** Fielded with U.S. Army and U.S. Forces Korea (now known as "Phrasalator")

■ **Joint Warning and Reporting Network (JWARN):** Successfully conducted spiral development; completed Joint Systems Integration Command (JSIC) planned assessment as part of Deployable Joint Command and Control (DJC2) Global Command and Control System

(GCCS) 4.0 interoperability demonstration

■ **Advanced Geospatial Imagery Library Enterprise (AGILE):** National Geospatial-Intelligence Agency (NGA) operational capability development initiative; assessed by JSIC as an integral part of the Joint Baseline Assessment for transmitting imagery; highlighted in Signal Magazine, March 2007, as providing, "...U.S. Air Force combat forces access to advanced imagery solution that allows large, high-resolution files to be shared at high speed over low bandwidth."

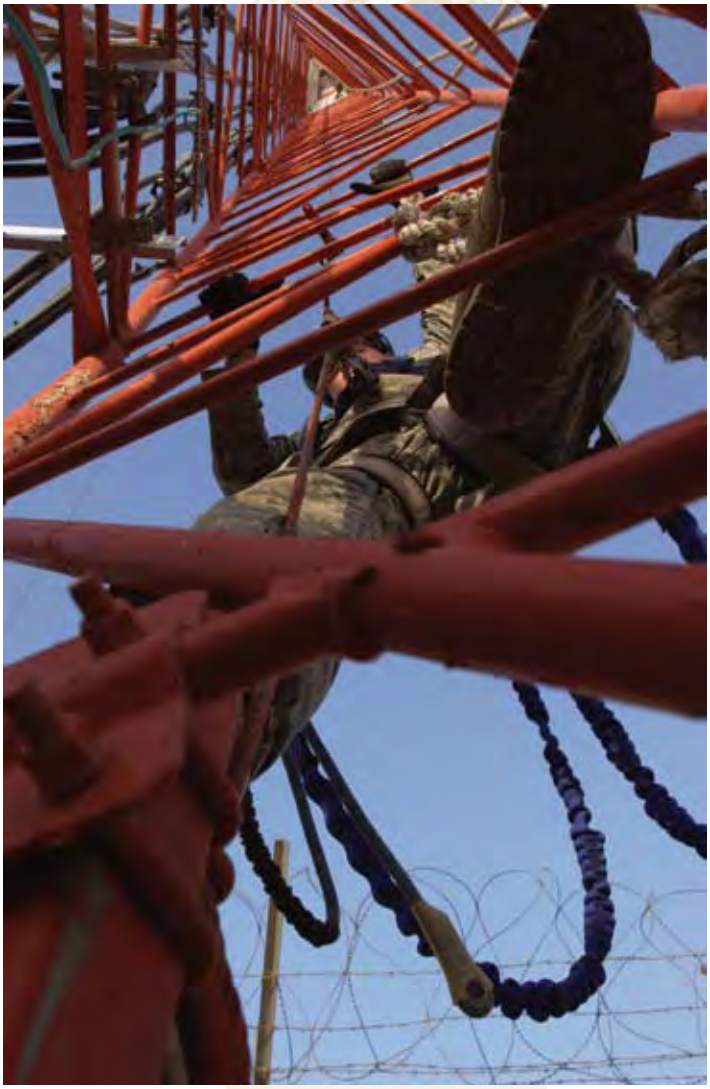
■ **Radiant Mercury Guard (RMIG):** Fielded with U.S. Navy; facilitates secure communications

■ **Common Operational Modeling, Planning and Simulation Strategy (COMPASS):** Demonstrated in 1996; fielded with combatant commands in 1998 for Bosnia-Herzegovina operations; inspired current common operational picture utilities

■ **Posted Applications Over Return Channel Satellite:** Global Broadcast System (GBS) spiral development of operational communications program of record (POR)

■ **Commercial Joint Mapping Tool Kit (CJMTK):** NGA POR: continues spiral development; currently fielded in support of joint operations

■ **Defense Collaborative Tool Suite (DCTS):** Collaboration suite; deployed to Afghanistan for Operation Enduring Freedom; subsequently designated DoD standard tool set for collaboration.



■ **Mobile Tactical Edge Network (MTEN):** NORAD-USNORTHCOM sponsored; developed to enable information sharing at strategic, operational and tactical levels for military, agency and coalition; provides remote access to classified and unclassified enclaves

■ **Integrated Information Management System (IIMS):** U.S. Air Force and U.S. Army sponsored; scalable system that supports a common operational picture for commanders and geographically separated unit control centers; spiral development effort in support of transition agreements with the Joint Warning and Reporting Network POR

■ **Scalable Mesh Networks:** Canadian sponsored; developmental communications protocol creating a large, self-forming and self-healing network using very low bandwidth radios; BFT applications with up to 1000 nodes

GENERAL OBJECTIVE:

Cross-domain and multi-security level data exchange tools

■ **NetTop:** U.S. Navy sponsored; purchased by Commander 3rd Fleet, recommended for funding/fielding and is currently a 2007 Cross Domain Solution Baseline technology

■ **Coalition Assured Sharing Environment (CASE):** Defense Information Systems Agency (DISA) sponsored; data separation within and between security domains to support multiple communities of interest (COIs) information sharing requirements

■ **Assured File Transfer (AFT):** National Security Agency (NSA) sponsored; enables secure transfer of high risk, complex files bi-directionally between domains of varying security classifications

■ **Joint Strike Fighter Off-board Mission Support Environment (JSF OMSE):** U.S. Air Force sponsored spiral development of Joint Strike Fighter (JSF) mission planning software that fulfills U.S. and JSF partner collaboration

■ **Italian Navy Maritime Command & Control Information System (MCCIS-Italy):** Italian Maritime command and control (C2) system; demonstrated and fielded to support maritime commanders and staff personnel by automatically acquiring and maintaining information for display and analysis; conforms to GCCS-J and Air Tasking Order (ATO) data formats

■ **Multi-National Coalition Security System (MNCSS):** Canadian sponsored technology: Microsoft Rights Management Services for classification of electronic correspondence; purchased/adopted by U.S. Central Command (USCENTCOM) for encryption-decryption

■ **Multi-level-secure Information Infrastructure (MI2):** Security certification programmed for 2008 completion; may lead to participation as DISA Combined Enterprise Regional Information Exchange (CENTRIX) Cross Enclave trial

■ **Coalition Information Assurance COP (CI-A COP):** First multi-domain coalition network infrastructure as part of an Advanced Concept Technology Demonstration (ACTD)

GENERAL OBJECTIVE:

Integrated logistics planning and coordination tools

■ **Contingency Theater Automated Planning System (CTAPS):** Fielded by the U.S. Air Force for inter-service use; key support for air, sea and land coordinated strike planning and live mission deconfliction

■ **Tactical Medical Coordinating System (TacMedCS):** U.S. Marine Corps Warfighting Laboratory spiral development initiative; limited fielding for current operations

■ **Intelligent Road/Rail Information Server (IRRIS):** U.S. Army POR; government owned; expanded utility to U.S. Transportation Command.

GENERAL OBJECTIVE:

Enhance government agency interoperability

■ **Collaborative Information Exchange Environment (CIEE):** National Guard Bureau POR; continues spiral development as Joint Collaborative Information Exchange Environment

■ **Wide Area Interoperability System (WAIS) & ACU 1000):** NORAD-USNORTHCOM sponsored; available on GSA schedule; Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA) and U.S. Coast Guard purchased technology as core of Mobile Disaster Vehicles communications suite

■ **Incident Commander's Radio Interface (ICRI):** NORAD-USNORTHCOM and civil law enforcement activities purchased technology in support of Homeland Security/Homeland Defense (HS/HD); U.S. Marine Corps installed in Rapid Response Vehicles to interface with civil authorities for crisis response; used effectively following hurricane Katrina; 2008 limited fielding with the U.S. Navy Small Boat Division

■ **ARINC Wireless Interoperability Solution (AWINS):** Supported hurricane Katrina relief effort; fielded as primary communications-integration system employed by the Maryland Transit Administration Emergency Response Vehicles

■ **Area Security Operations Command and Control (ASOCC):** Limited fielding in support of U.S. Army interoperability with DHS, Justice (DoJ) and Defense (DoD) departments

■ **Rapid Response System-Deployable (RRS-D):** Fielded by U.S. Marine Corps; provided criti-